

Novel Approaches to Applied Cyber Security in Privacy, Encryption, Security Systems, Web Credentials, and Education.

Rodrigo Ruiz (Rodrigo de Souza Ruiz, Natasha Ruiz)

ORCID 0000-0003-1644-3933

Submitted in partial fulfilment of the award of Doctor of

Philosophy by Prior Output

Intelligent Systems Research Centre

School of Computing and Digital Media

London Metropolitan University

Supervisors:

Prof. Dr. Hassan Kazemian

Dr. Pancham Shukla

London, 2022

Statement of Originality

This narrative commentary and the research outputs listed in Appendix U have been submitted in partial fulfilment of the requirements for the PhD award by Prior Output at Intelligent Systems Research Centre, School of Computing and Digital Media, London Metropolitan University. Both the commentary and the outputs are the sole work of the candidate. No part of this submission, including outputs, narrative, and appendices, has previously been submitted for award elsewhere.

Acknowledgements

The guidance of my supervisors Professor Hassan Kazemian and Dr. Pancham Shukla made this submission possible. I am thankful for Professor Hassan Kazemian to give me the opportunity and grateful for Dr. Shukla to spent a lot of time with me. Also, I am thankful for the support during my career as my colleagues of CTI Renato Archer, Amândio Balcão Filho, Dr. Ferruccio de Franco Rosa, Kil Jin Brandini Park Dsc, Dr. Antônio Montes, Dr. Rodrigo Bonacin, Dr. Victor Mammana, and my friend and partner of research from Brazilian Army, Cel. Rogério Winter. Thank you for a soul that shares my body and share this journey, Natasha Ruiz. Thank you, my mother, Roseli Ruiz, for her support. I thank Victoria Ganzert, love of my life for her moral support, encouragement, and financial support during my life journey. Special thanks to my son Tyler and my daughter Ivy for the joy they bring to my heart.

Abstract

This work is inspired by Brazilian Government cyber security needs for industry, government and people. It is divided in five elements: Privacy, Encryption, Web Credentials, Security Systems and Education.

The right to privacy has been widely debated in many countries because of the implications that threaten people, civil liberties and the right to citizenship. Since 2018, GDPR has been in force in the EU and has been a milestone for people and institutions' privacy. On **Privacy**, this work presents with four research papers and three versions of a method to restore *InPrivate* or *incognito* navigation over IE, Edge, Firefox, Chrome, Safari, Opera and TOR able to expose all navigation made over *incognito* mode.

The secrets of different companies, countries and armed forces are entrusted to encryption technologies. On **Encryption**, this work provides three methods in three research papers to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods.

Credentials are data that give someone the right to access a location or a system. They usually involve a login, a username, email, access code and a password. Biometrics is used in some critical operations but still insipient. **Web Credentials** was explored in one research paper and it shows how to get the completely fully clear text of user credentials after the analyst having access to the computer target. The proposed method can get credentials used in intranets or e-commerce; home banking and email accounts. The Brazilian federal bank Caixa Econômica Federal improve its home banking because of this research. It is a biggest bank in Brazil and every Brazilian uses

their social services.

Antimalware systems have been deployed for protecting information systems for decades. On **Security Systems** this work was presented methods to create a cyber autoimmune disease and scenarios analysis to use it over military demands. This research demonstrates the use of harmless DNA fragments extracted from computer viruses from the 80's and their use to induce an autoimmune cybernetic disease capable of fooling the most famous antiviruses. These systems made for protection, if induced by this method thus cause a complete destruction of the operating system and a loss of customer data.

The human factor will always be the most important and at the same time the most flawed and dangerous. Cybersecurity's primary awareness is expected through University education, but the academic discourse is often dissociated from practice. On **Cyber Security Education**, this research provides in two research papers, a critical survey of cyber security education that explores UK Undergraduate Computer Science curricula and shows that cybersecurity as an optional content at the end of the course. Also, this research proposes a method to classify how relevant is cyber security in this environment. The method presents a new insight into cybersecurity education. IRCS Index of Relevance in Cybersecurity (IRCS) intends to classify the computer science courses offered in UK Universities based on the relevance of cybersecurity formal presented in their curricula.

This research is innovative, as it presented topics related to the areas of technology, processes, people and usage environment. It shows practical solutions to complex problems facing the armed forces, governments, Cyber Security professionals and society. Also it specifically contributes to military strategy scenarios in cyber warfare and investigative work in digital forensics labs and academia.

Table of Contents

Statement of Originality	2
Acknowledgements	3
Abstract	4
Table of Contents	6
Figure Index	10
Table Index	12
Abbreviations	16
1. Introduction	18
1.1. Research Problem	22
1.2. Motivations	22
1.3. Contribution to Knowledge	23
1.4. Thesis Structure	30
2. Literature review about Privacy, Encryption, Security Systems, Web Credentials, and Cyber Security Education	31
2.1. Literature review about Privacy	38
2.2. Literature review about Encryption	46
2.3. Literature review about Web Credentials	49
2.4. Literature review about Security Systems	52
2.5. Literature review about Cyber Security Education	55
3. Research Methodology	60

3.1.	Privacy	60
3.2.	Encryption	65
3.2.1.	Truecrypt	65
3.2.2.	Bitlocker and BitDefender Total Encryption	68
3.2.3.	PGP Symantec Encryption Desktop SED	71
3.3.	Security Systems	73
3.3.1.	Apoc@lypse Technique	74
3.4.	Web Credentials	77
3.5.	Cyber Security Education	81
3.5.1.	Cyber Security Education in UK Computer Science Courses	82
3.5.2.	IRCS (Index of Relevance in Cyber Security)	83
4.	Privacy	88
4.1.	Introduction	88
4.2.	Author's Contributions to Privacy	89
4.3.	Summary	93
5.	Encryption	94
5.1.	Introduction	94
5.2.	Author's Contributions to Encryption	95
5.3.	Summary	99
6.	Web Credentials	101
6.1.	Introduction	101

6.2.	Author's Contributions to Web Credentials	103
6.3.	Summary	105
7.	Security Systems	107
7.1.	Introduction	107
7.2.	Author's Contributions to Security Systems	113
7.3.	Summary	118
8.	Cyber Security Education	120
8.1.	Introduction	120
8.2.	Author's Contribution to Cyber Security Education	121
8.3.	Summary	123
9.	Discussion	125
9.1.	Privacy	125
9.2.	Encryption	129
9.3.	Security Systems	132
9.4.	Web Credentials	136
9.5.	Cyber Security Education	138
9.5.1.	Cyber Security Education in UK Computer Science Courses	138
9.5.2.	IRCS (Index of Relevance in Cyber Security)	142
10.	Conclusion	144
11.	Future Work	148
	References	150

Appendix A Metrics	166
Appendix B Other Academic and Social Contributions	173
Appendix C: Research Background	184
Appendix D: Specialist Diploma	188
Appendix E: Recommendation Letter, Professor Abdul Razaque	191
Appendix F: Recommendation Letter, Dr Mauro Coimbra	192
Appendix G: Recommendation Letter, Dr Jarbas Cardoso	193
Appendix H: Recommendation Letter, Dr Ferrucio Rosa	194
Appendix I: Recommendation Letter, SDIWC	195
Appendix K: Recommendation Letter, Bob Miko	196
Appendix L: Recommendation Letter, Julia Dolengo	197
Appendix M: Recommendation Letter, Lorival Moreira	198
Appendix N: Invitation to Keynote Speaker	199
Appendix O: Invitation to Comment on Cyber Security to International Media	200
Appendix P: Amazon top 100 UK (Ruiz, et al., 2015)	201
Appendix Q: Amazon top 10 Germany (Ruiz, et al., 2015)	202
Appendix R: Invitation to Publish a Book	203
Appendix S: Chair of International Conference	204
Appendix T: Declarations of Co-writers	205
Appendix U: Full Text of Prior Outputs Submitted For Award	208

Figure Index

Figure 1 Relation of dependence. This inverted pyramid according to the vision of the author presents how Cyber Security education sustains the entire system.	21
Figure 2 MTTR	28
Figure 3 Heat map of words and expressions used in the outputs.	29
Figure 4 - Discovery Channel web page accessed with Windows Edge in private mode navigation.	126
Figure 5 - Data recovered after a system reboot. All data on the Discovery Channel web page was recovered.....	127
Figure 6 Truecrypt screen to generate encrypted volume.	66
Figure 7 Bit Defender Total Encryption.....	69
Figure 8 - BitDefender footers file comparison. In the A empty file with the password 123456789 and at B encrypted data with another password.....	70
Figure 9 - The figure shows encrypted data was exposed by using the method with a deprecated password.	70
Figure 10 - Visual representation of a method to use deleted users to having access to actual encrypted data with PGP.....	72
Figure 11 - NASA screenshot with instructions about use PGP file encryption.....	97
Figure 12 - Citi bank home banking	81
Figure 13 - Gmail full opened credentials.....	104
Figure 14 - Injection methods.	75
Figure 15 - In Portuguese, the Avast shows the message "The module Files of Avast! was blocked a Theat. No actions are necessary" free translation by the author.....	117
Figure 16 - In Portuguese, after Avast conclude the service " The computer can't be	

initialized."	76
Figure 17 - In this case, Norton has destroyed all program files.	77
Figure 18 - Human system of protection resume. (Ruiz, et al., 2015)	

133

Figure 19 - Correlation of human protection system with cyber protection system. (Ruiz, et al., 2015).....	133
Figure 20 Considering 100 Computer Science Courses, Security as an optional discipline or an element of other disciplines on the UK computer science courses. 61% have security on the curriculum and 39% have no security on the curriculum. (Ruiz, 2019)	Erro! Indicador não definido.
Figure 21 Considering the total contents 189 under 100 Computer Science Courses, Security as a mandatory discipline or an element of other disciplines on UK computer science courses. 6% of courses have no security content on the curriculum and 54% of courses have mandatory Cyber Security elements on the curriculum and 40% have optional security content. (Ruiz, 2019)	Erro! Indicador não definido.
Figure 22 Considering the total 189 security content, Security discipline's distribution by year on UK computer science courses. 17% focus on security content in the first year, 23% in the second year, 60% in the third year or later. (Ruiz, 2019)	Erro! Indicador não definido.
Figure 23 - Researchgate statistics of the School of Computing of London Metropolitan University.	171
Figure 24 The Researchgate score is indicative of the paper's relevance.	172
Figure 25 Google Scholar statistics	172

Table Index

Table 1 Published contributions by cyber security element between 2011 and 2021.	22
Table 2 Published work review, classification and selection for submission for Award.	25
Table 3 Average investment in Cyber Security in the last financial year (UK). Source (Department for Digital, 2019)	33
Table 4: Test Types	64
Table 5 - In private mode test results.	92
Table 7 - Signatures	78
Table 8 Setup test	79
Table 11 - Collected data extracted by reading course descriptions provided by each institution on their own curricula description. (Ruiz, 2019)	83
Table 6 - Tested sites.	102
Table 9 Apoc@lypse method, a sequence of events: an antivirus action.	134
Table 10 Spent on Cybercrime as a Percentage of the GDP (Source: Intel Security (Studies, 2014))	135
Table 12 IRCS - Index of Relevance in Cyber Security 2019, dataset.	85

Figure Index

Figure 1 Relation of dependence. This inverted pyramid according to the vision of the author presents how Cyber Security education sustains the entire system. 21

Figure 2 MTTR 28

Figure 3 Heat map of words and expressions used in the outputs. 29

Figure 6 Truecrypt screen to generate encrypted volume. 66

Figure 7 Bit Defender Total Encryption 69

Figure 8 - BitDefender footers file comparison. In the A empty file with the password 123456789 and at B encrypted data with another password. 70

Figure 9 - The figure shows encrypted data was exposed by using the method with a deprecated password. 70

Figure 10 - Visual representation of a method to use deleted users to having access to actual encrypted data with PGP. 72

Figure 11 - NASA screenshot with instructions about use PGP file encryption. 97

Figure 14 - Injection methods. 75

Figure 15 - In Portuguese, the Avast shows the message "The module Files of Avast! was blocked a Theat. No actions are necessary" free translation by the author. 117

Figure 16 - In Portuguese, after Avast conclude the service " The computer can't be initialized."76

Figure 17 - In this case, Norton has destroyed all program files. 77

Figure 12 - Citi bank home banking 81

Figure 13 - Gmail full opened credentials. 104

Figure 4 - Discovery Channel web page accessed with Windows Edge in private mode navigation. 126

Figure 5 - Data recovered after a system reboot. All data on the Discovery Channel web page was recovered. 127

Figure 18 - Human system of protection resume. (Ruiz, et al., 2015) 133

Figure 19 - Correlation of human protection system with cyber protection system. (Ruiz, et al., 2015) 133

Figure 20 Considering 100 Computer Science Courses, Security as an optional discipline or an element of other disciplines on the UK computer science courses. 61% have security on the curriculum and 39% have no security on the curriculum. (Ruiz, 2019) 139

Figure 21 Considering the total contents 189 under 100 Computer Science Courses, Security as a mandatory discipline or an element of other disciplines on UK computer science courses. 6% of courses have no security content on the curriculum and 54% of courses have mandatory Cyber Security elements on the curriculum and 40% have optional security content. (Ruiz, 2019) 140

Figure 22 Considering the total 189 security content, Security discipline's distribution by year on UK computer science courses. 17% focus on security content in the first year, 23% in the second year, 60% in the third year or later. (Ruiz, 2019) 141

Figure 23 - Researchgate statistics of the School of Computing of London

Metropolitan University. 171

Figure 24 The Researchgate score is indicative of the paper's relevance. 172

Figure 25 Google Scholar statistics 172

Abbreviations

ACM Association for Computer Machinery

CISCO Computer Information System Company

CTI Information Technology Centre

DIMEC Infrastructure Division for Mechatronic and Electronic Systems

DC District of Columbia

DNA Deoxyribonucleic Acid

DOD Department of Defence - United States

EICAR European Institute for Computer Antivirus Research Test File

ERP Enterprise Research Planning

FBI Federal Bureau of Investigation - United States

FED Full Encryption Disk

G400 Universities and Colleges Admissions Service code for Computer
Science Course

H-INDEX Index for measure scientific impact of publications considering
citations

HTTP HyperText Transfer Protocol

I10-INDEX Index for measure scientific impact of publications considering
citations

ICCICS International Conference on Cyber-Crime Investigation and
Cyber Security

ICCYBER International Cyber Crimes Expert Conference - Brazil

ICGS3 3th International Conference on Global Security, Safety, and Sustainability, London

INFOSEC International Conference on Information Security and Cyber Forensics

IRCS Index of Relevance in Cyber Security

IT Information Technology

NASA National Aeronautics and Space Administration

PGP Pretty Good Privacy

PhD Doctor of Philosophy

R2K Rodrigo, Rogério and Kil

SED Symantec Encryption Desktop

SIGE Symposium on Operational Applications in Defence Areas - Brazil

SSG15-044 Internal Code of Symantec Corp. to identify security case

UK United Kingdom

UNICAMP State University of Campinas, SP, Brazil

US United States

1. Introduction

Some principles of Cyber Security, like Privacy, Web Credentials Management, Encryption and Cyber Security Education are elementary and accompany modern society in all its activities. During the ten years of research synthesized in this thesis, the author analysed some principles and their foundations that include chapters in these works where they are raised. This work is inspired by Brazilian Government cyber security needs for industry, government and people. It is divided in five elements: Privacy, Encryption, Web Credentials, Security Systems and Education.

Business rules imbibed in software can affect privacy. Cyber Security is an essential part of computer science, and in the beginning, it was the goal of the first published articles by the author.

According to (Rosa, et al., 2018) there are various kinds of tests, e.g., Functional, Penetration, Fuzzing, Fault or Defect Injection, and

Exploratory. Verification is the activity aimed at verifying whether a requirement is present without a test of the functionality. This kind of verification is conducted in this work.

This research intends to present the candidate's prior publications demonstrating a coherent, connected, and in-depth line of selected outputs that affect privacy and Cyber Security. Those published work studies Cyber Security considering the technical, environment, process, and social aspects. This research also explains how the relevant papers form a coherent body of work, demonstrates methodological and conceptual rigour, and articulates the original academic contribution to the field of Cyber Security and the importance of contribution to British society.

To show the relevance of work will be provided with a list of outputs, abstracts, contributions, and citations in the Cyber Security field in Appendix A Metrics.

The publications below always explore the technical, environmental, process, and social aspects of Cyber Security.

Technical: The software and tools themselves, their code, and their functionality are analysed according to what their manuals define;

Environment: Analysing the environment is fundamental. Military, public, business, or personal. Each has its needs and challenges;

Process: The processes define the way each element is connected and is a fundamental part of the use of any software;

Social: Social or personal aspects are the key to everything. After all, processes and technology are developed by people for people. Besides, people control, modify and are directly affected by the environment.

The current Cyber Security paradigm is the training of more and more Cyber

Security specialists. Every year around the world, new courses are created to form Cyber Security specialists. This work confronts this reality by proposing different applied Cyber Security approaches in education, privacy, and systems.

For this reading, it is necessary to present how the author's name may have been published in several works: **Rodrigo Ruiz, R. de S. Ruiz, Rodrigo de S. Ruiz, Rodrigo de Souza Ruiz, Natasha de Souza Ruiz or Natasha Ruiz.**

According to (Strate, 1999) *“The term “cyberspace” is characterized by a multiplicity of meanings... cyberspace as a paraspace or nonspace, as well as the concept of cyberspacetime”* and others authors like (Olagbemi, 2014) try to redefine cyberspace to incorporate the role of the human actor and proposes a triad: human, application, and infrastructure dimensions.

Suppose if consider that the most critical, most prosperous, and most influential companies in the software market as involved in my research expose. These companies seek to hire the best professionals. Even though these professionals, in general, come from the best universities. It makes perfect sense to question the actual concepts and curricula. In analyzing the relation of the interdependence between entities of the Cyber Security presented in Figure 1 as vision of author after 30 years working with software, this work will explore two points of vulnerability:

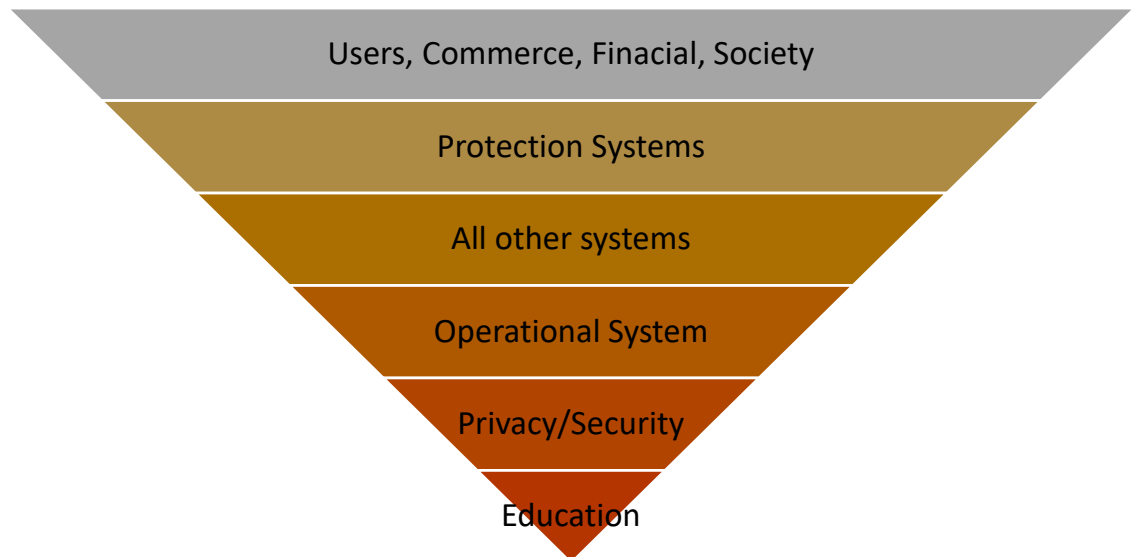


Figure 1 Relation of dependence. This inverted pyramid according to the vision of the author presents how Cyber Security education sustains the entire system.

The first is a historical and financial issue that has been with us since the first software until today. The concept of security in software was to emerge much later than the software history.

The second reflection is the cost of redesign actual software. It is not correct to blame the pioneers for having developed unsafe systems. The threats came to exist organically with the opportunities created by the new software and mainly with the popularization of these systems. The creators and directors of two of the biggest security software companies have publicly declared that their products are useless because they are unable to protect the user against a large number of threats (Gibbs, 2014) (McAfee, s.d.). The choice of an inverted pyramid Figure 1 aims to reinforce all these small environment' instability and the responsibility of the educational system for a better future in the cybernetic area. Programming safe since the first line of the first code is the best choice for better Cyber Security in the next decades.

As seen in Table 1 this research was distributed into five elements of cybersecurity: Privacy, Encryption, Web Credentials, Security Systems and Education. Table 1 show some metrics of the contribution. Each element haves its chapter and the

contribution and explanation of methods and Scenario Analysis are detailed.

Table 1 Published contributions by cyber security element between 2011 and 2021.

Cyber Security Element	Method	Scenario Analysis
Privacy	3	1
Encryption	3	2
Web Credentials	1	1
Security Systems	2	3
Education	1	1

1.1. Research Problem

World Economic Forum are correct electing Cyber Security a big problem (World Economic Forum, 2018) for short and medium time, together with climatic changes. The author is oriented over a decade by the Brazilian government to provide the best cyber security to people, government, Army and financial system. To support this demand, this research focused on exploring five Cyber Security elements: privacy, encryption, web credentials, security systems, and Cyber Security education.

1.2. Motivations

The motivation behind this research is the global concern about the impacts that cyber threats having increasing in the actual world. Today person's life is influenced by software. Business, health, education, communications and fun time. Also the defences and economy of the Globe too. Computer science is a new field in comparison to other sciences and was start concerned with practical aspects. Cyber threats appear for the first time just in 1988 (NATO, s.d.) 40 years after the first software (Burton, 2005). Cyber security concept appeared with a minimum of four decades of lack, and since then, the software industry has been patching each of the various holes that appear without ever promoting structural change. The first time, the

Economic World Forum (World Economic Forum, 2018) put Cyber Security on top World threat, side by side with human problems like climatic changes. In 2019 more than 24 million unique malware are identified. Note it is just the number that antivirus companies can identify. (CSO, 2020) It is a big number, and according to (Crane, 2020) USD3.5Billions were lost by the world in 2019. UK Government has produced an essential survey in 2019 (Department for Digital, 2019) about Cyber Security and got some anonymous comments:

“Cyber Security is one in a long list of costs of doing business, so no-one's going to get excited about it unless you have regulatory focus.” **Large business**

As a global issue, this UK survey shows that it is an Estate problem. For Large businesses, it is just a cost problem.

1.3. Contribution to Knowledge

In 16 prior publications presented in Table 2, the author provides 11 Methods and 8 Scenario Analyses distributed in Privacy, Security Systems, Encryption, Web Credentials, and Cyber Security Education. Each contribution will be detailed during the text, and this section will be explored some metrics. Appendix A presents more metrics and details about citations.

Table 2 contains a list of contributions. The order of table considers by first the non-self cited, Google Scholar¹, and after Researchgate².

Table 1. with the legend:

Id - Identification number attributed by reading order;

¹ <https://scholar.google.com/citations?user=CrINQVwAAAAJ&hl=pt-BR&oi=sra>

² https://www.researchgate.net/profile/Natasha_Ruiz

Submitted for Ward – Yes or no if the output is the part of the thesis;

Title - Refers to the title of the published article;

Year - The year of publication;

Type- Publication type:

(C) The conference, (J) Journal, (B) Book, (M) Magazine or (BC) Book Chapter;

Contribution: This field intends to show the principal contribution as (MD) Method or (SA) Scenario Analysis;

Citations by: Google, Researchgate and extracted Self Citation

Language - Language refers to the language in which the article was published: (P) Portuguese language or (E) English language;

Reference – Reference citation.

Table 2 permits visualization of my published work in the Cyber Security field, and it is ordered by publish year to easy location when referred in text and to demonstrate the evolution of the research during my career. The summarization is presented during the text in chapters 3,4,5,6 and 7. Only outputs selected for submission for the award are displayed in Table 2.

Table 2 Published work review, classification and selection for submission for Award.

Id	Submitted for Award	Cyber security element	Year	Contribution	Type	Citations			Title and local of publication
						Google	ResearchGate	Non-self cit.	
1	yes	Privacy	2012	MD	C		4		Turning Public the private navigation. Tornando Pública a Navegação "In Private" (Rodrigo de S. Ruiz et al., 2012) ICCYBER (International Cyber Crime Expert Conference 2012) fully presented in Appendix U
2	yes	Privacy	2014	MD	C	3	3	2	Opening the " Private Browsing " Data - Acquiring Evidence of Browsing Activities (Ruiz, et al., 2014) The International Conference on Information Security and Cyber Forensics (InfoSec2014) fully presented in Appendix U
3	yes	Encryption	2014	MD, SA	C	2	2		Security Issue on Cloned TrueCrypt Containers and Backup Headers (Rodrigo de S. Ruiz et al., 2014) The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014) is fully presented in Appendix U
4	yes	Security Systems	2015	SA	C		1		Apoc@lypse: when the anti-malware is sick (Ruiz & Winter, 2015) Cyber Defence Magazine, 2015 pages 26-28 fully presented in Appendix U
5	yes	Security systems	2015	MD	B		2		Apoc@lypse: The end of antivirus (Ruiz, et al., 2015) Book published in 2015 ISBN 9781514863671 http://dl.acm.org/citation.cfm?id=2876178 partial presented in Appendix U
6	yes	Privacy	2015	MD	J	9	9	12	Overconfidence: Personal Behaviour s Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode (Ruiz, et al., 2015) Journal of Cyber Security and Digital Forensics, 2015 pages 404-416 fully presented in Appendix U
7	yes	Encryption	2016	MD, SA	M	2	3		Corrosive Secrecy And Confidence: The Paradox Among Bypassing Cryptographic Software (Winter & Ruiz, 2016) Cyber Security Review, Spring 2016 pages 66-74 fully presented in Appendix U
8	yes	Security Systems	2016	SA	M				Apoc@lypse: The End Of Antivirus. When The Antivirus Is The Threat (Winter & Ruiz, 2016) Cyber Security Review, Spring 2016 pages 58-65 fully presented in Appendix U
9	yes	Encryption	2016	MD	J	1	2		Lazarus: Data Leakage with PGP and Resurrection of the Revoked User (Ruiz & Winter, 2016) Journal of Cyber Security and Mobility, 2016 V5-2 pages 1-14 fully presented in Appendix U

10	yes	Security Systems	2017	SA	M				Cyber Security, Cyber Weapons And Cyber-Attacks: Responsibility And Different Reflections (Winter & Ruiz, 2017) Critical Infrastructure Protection Review Magazine, 2017 V2 pages 77-82 fully presented in Appendix U
11	yes	Web Credentials	2017	MD, SA	J	4	3	2	The leakage of passwords from home banking sites: A threat to global Cyber Security? (Ruiz, et al., 2017) Journal of Payments Strategy & Systems Volume 11 Number 2 pages 1-13 fully presented in Appendix U
12	yes	Security Systems	2017	MD	J		2	1	Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life (Winter & Ruiz, 2017) International Journal of Cyber Security and Digital Forensics Vol 7, 1 pages 21-30 fully presented in Appendix U
13	yes	Education	2019	SA	C	2	1	2	A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cyber Security (Ruiz, 2019) IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) pages 1-8 fully presented in Appendix U
14	yes	Privacy	2020	SA	J				Privacy in The First Line of the First Code (Ruiz, et al., 2020) E-Letter Science Magazine https://science.sciencemag.org/content/317/5842/1178/tab-e-letters fully presented in Appendix U
15	yes	Education	2020	MD	J				Cyber Security Index For Undergraduate Computer Science Courses in the UK (Ruiz, et al., 2020) Journal of Applied Security Research https://www.tandfonline.com/doi/10.1080/19361610.2020.1798173 fully presented in Appendix U
16	Yes	Education	2021	MD	C				Method and Tool for Generating Table of Relevance in Literature Review (MTTR), 22 nd European Conference on Knowledge Management ECKM 2021 DOI: 10.34190/EKM.21.199, Coventry University, 2021, Fully presented in Appendix U

MD=Method, SA=Scenario Analysis, J= Journal, C=Conference, M=Magazine, B=Book

Another kind of relevance is economic and social relevance. The work was responsible for changing several Brazilian banks' home banking, with millions of customers being protected. The works about bypass in cryptography (Ruiz & Winter, 2016) (Rodrigo de S. Ruiz et al., 2014) (Ruiz & Winter, 2016) (Ruiz & Winter, 2016); private browsing (Rodrigo de S. Ruiz et al., 2012) (Ruiz, et al., 2014) (Ruiz, et al., 2015) (Ruiz, et al., 2017) and antivirus systems, (Ruiz, et al., 2015) (Winter & Ruiz, 2016) (Winter & Ruiz, 2017) (Winter & Ruiz, 2017) (Montes, et al., 2014) were responsible for the invitation, to speak at various professional and academic events,

including postgraduate courses.

In each research, researchers in computing, IT and all other fields are challenged with several articles that they need to rate, classify and separate quickly and effectively to contextualize and further advance their research effectively. It is considered that literature review is the most important step of discovery. Notably, a literature review allows the researcher to adjust the perspectives and limitations of an area of study. Though, there is a absence of effective methods and tools for this activity. Often, traditional knowledge management methods result in the “Gordian Knot” slowing down the process of literature review considerably. To make this effort more easy this author and co-authors, prose the Method and Tool for Generating Table of Relevance in Literature Review (MTTR).

The anecdotal evidence reported suggests that it is possible to carry out a literature review in a much shorter time with MTTR than in the traditional manner. Until the traditional methods are exclusively subjective and exhaustive to do. The MTTR presented in Figure 2 provides an objective analysis and its results can be used before the systematic review. In this case the researcher will read the most relevant paper.

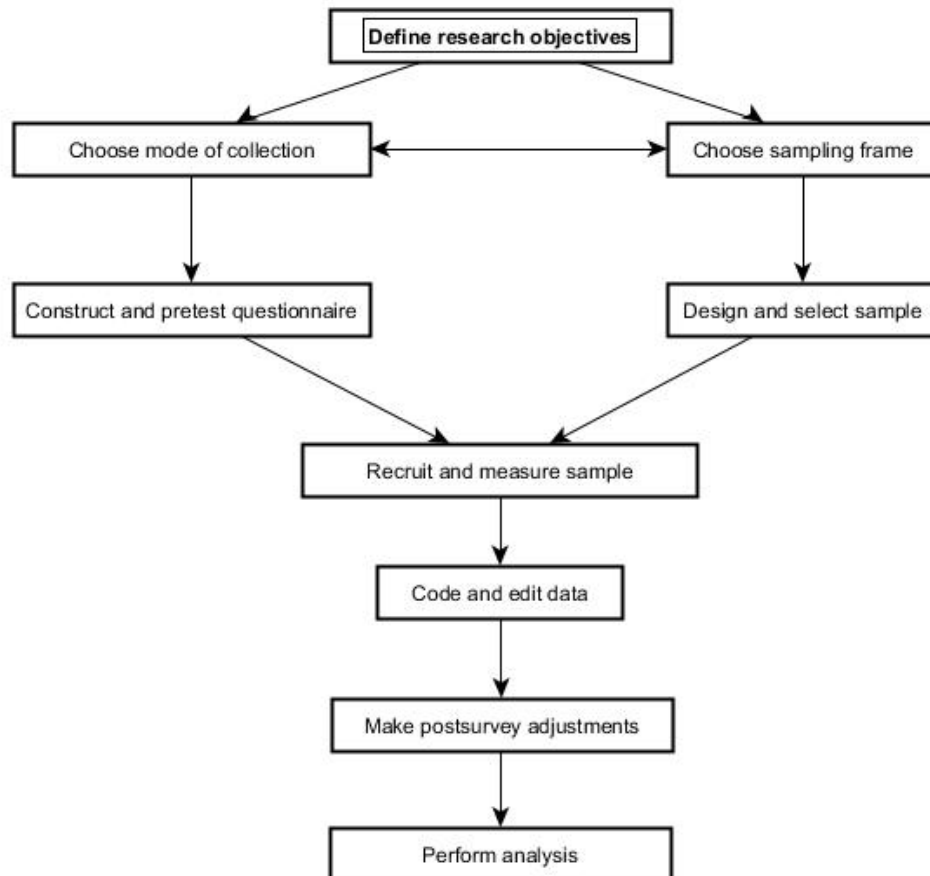


Figure 2 MTTR

The MTTR is an innovative organizing method supported by software tools that make the literature review activity more efficient, faster and cheaper. An interesting feature of MTTR is data visualization using the Heat Map technique, Word Cloud and statistical techniques in designating and comparing each scientific article with the other relevant articles. The productivity gains in MTTR occur due to the automation in structuring and sorting scientific articles. In addition to efficiency, the lowest cost has the potential to place the MTTR as a preferred tool for the researcher.

As a sample Figure 3 show the results of MTTR when it process the published works present in this thesis.

Articles	(Ruiz, et al., 2015)	(Ruiz, et al., 2015)	(Winter & Ruiz, 2016)	(Winter & Ruiz, 2017)	(Ruiz, 2019)	(Ruiz, et al., 2017)	(Winter & Ruiz, 2016)	(Rodrigo Ruiz, 2017)	(Ruiz, et al., 2014)	(Ruiz, et al., 2020)	(Ruiz, et al., 2020)	(Ruiz & Winter, 2015)	(Winter & Ruiz, 2017)	(Ruiz, et al., 2012)	total
system	208	34	25	71	12	23	54	17	5	8	0	14	33	21	525
security	66	0	58	0	77	30	22	30	13	0	54	6	0	1	382
file	72	35	27	43	7	18	13	41	59	17	5	0	5	0	342
antivirus	214	0	1	43	0	0	40	0	0	0	1	3	12	2	316
data	42	38	22	5	23	40	8	35	29	28	8	13	0	6	308
user	66	26	14	12	26	22	0	36	19	18	19	21	2	0	284
software	87	18	46	6	26	0	6	22	17	1	13	22	10	4	278
information	51	0	44	0	17	36	17	25	19	0	0	4	16	0	229
attack	27	2	28	19	2	23	32	8	22	0	3	6	2	25	199
cybersecurity	12	0	4	7	50	0	10	15	0	0	42	16	0	13	169
browser	2	74	0	0	7	27	0	0	0	36	6	11	0	0	163
analysis	18	67	3	1	6	11	2	1	3	46	0	0	0	0	158
malware	87	0	0	22	0	5	20	0	0	0	0	0	21	2	157
virus	109	0	0	30	0	0	9	0	0	0	0	0	9	0	157
discovery	5	74	1	0	0	0	1	0	1	69	0	0	0	0	151
Privacy	1	39	6	1	20	3	1	16	2	6	18	13	0	2	129
cyber	0	0	0	0	0	0	51	0	0	0	0	0	5	61	117
method	26	17	11	9	1	10	5	12	11	7	2	2	1	0	115
Encryption	0	2	37	0	9	1	1	23	12	0	8	0	3	1	97
test	25	0	13	11	0	14	0	2	0	0	0	0	2	1	68
cyber security	0	0	7	3	8	5	6	2	0	0	13	6	1	4	55
cyber autoimmune disease	31	0	0	16	0	0	3	0	0	0	0	0	2	0	52
Education	1	0	0	0	19	1	1	0	0	0	21	3	0	0	46
cybersecurity education	0	0	0	0	2	0	0	0	0	0	3	0	0	0	5
total	1061	294	272	259	253	235	233	230	186	154	151	131	104	89	15

Figure 3 Heat map of words and expressions used in the outputs.

As seen in the outputs are sorted horizontally and vertically by the number of these words and expressions in the text providing a heat map of themes. It is a way to easily identify the specific them used by the authors in the text. Top and right indicate

more relevance in the specific use of a term like “security, system or antivirus”. Besides, at the bottom, the fields that represent new opportunities to study, taking into account that these 16 articles reviewed hundreds of other articles by other authors and the words and expressions used to reflect this analysis, the term “Cyber Security Education” is in the centre of this work. It uses the MTTR method. (Ruiz, et al., 2021)

These works also help vendors to improve more security and efficiency in their software for their users. It is possible to see contributions for the Brazilian Army and Brazilian Government in the process of software purchase with an honourable mention by the Brazilian Federal Court of Accounts³. Other work here is used to improve more privacy and security by vendors (Ruiz, et al., 2014) (Rodrigo Ruiz, 2017).

1.4. Thesis Structure

This thesis intends to facilitate the understanding and organization of all academic and professional works in the author's Cyber Security areas and this thesis is presented in eleven chapters, Introduction, Literature Review, Research Methodology, Privacy, Encryption, Web Credentials, Security Systems, Cyber Security Education, Discussion, Conclusion and Future Work. The author's background can be verified in Appendix A, P, and Q that show publication metrics, Appendix B that show others author contribution, Appendix C that shows author's cyber crime prevention diploma, Appendix E to M that shows reference letters, Appendix N, O, S that show invitations to be the speaker. Appendix T show's co-author declaration that co-working and finally Appendix U include the full text of all 16 papers submitted to award.

³ <https://tcu.jusbrasil.com.br/jurisprudencia/316046265/3733820110/inteiro-teor-316046287> search for keyword CCOMGEX

2. Literature review about Privacy, Encryption, Security Systems, Web Credentials, and Cyber Security Education

As this work addresses different Cyber Security aspects, it became more appropriate for each chapter to have its literature review. In this chapter, the review intends to introduce the reader to the themes that will be addressed and deepened in the following chapters.

According to (Sadok & Bednar, 2015) (Maclean, 2011) (Cebula & R.Young, 2010), the excessive use of technical focus is the principal of the reasons for deficiencies of Cyber Security, it is necessary to pay attention to people, methods and environment too. Systems are composed of people, processes, and technology. IT system is human interaction systems according to (Sadok & Bednar, 2015). It is more common that authors from Cyber Security and other areas include just three of these elements, the golden triangle: Technology, Process, and People. (Lewis & Nguyen,

2020) (Andress, 2013) (Cox, 2006). Another element is added in the interaction of Process, Technology and People. The Environment is symbiotic and does not occur separately (Rogério Winter et al., 2018).

To this work, the fourth element, the environment, is very relevant because it permits and regulates the interactions between the others elements. The same Cyber Security issue has different consequences when it is in a corporate, personal, or governmental environment. The total amount of damage when the issue affects an individual is low. Still, for the individual, the damage in the finance or private life can be devastating, including leading to suicide (AJ Willingham, CNN, 2019) (Tim Fitzsimons, NBC News, 2019) (Chris Baraniuk, BBC News, 2015). When the environment is corporative, the damage is about how much money is lost; industrial hacking is big business in the world. Banks and innovative industries are the preferred victims (Ruiz, et al., 2017). About the government environment, the damage can be the control of the state, money, or military (Ruiz & Winter, 2016) (Ruiz, et al., 2015) (Rogério Winter et al., 2018) (Rodrigo de S. Ruiz et al., 2014) (Rogério Winter et al., 2018).

Why is society having a sensation of insecure Cyber Security? It is possible to answer it, looking for some data and news.

In 2019, a total amount of 24,610,126 unique malware is identified. Note it is just the number that antivirus companies can identify (CSO, 2020). It is a big number, and according to (Crane, 2020) USD3.5Billions were lost by the world in 2019.

UK Government has produced an essential survey in 2019 (Department for Digital, 2019) about Cyber Security and got some anonymous comments from Large(big companies, normally global companies), Medium (normally national

companies) and Microbusiness (normally local and familiar business with less than 100 workers):

“Cyber Security is one in a long list of costs of doing business, so no-one's going to get excited about it unless you have regulatory focus.” **Large business**

“I would not say that I am the most informed person. It's not information I go out and seek unless I am aware of a specific threat then absolutely we do the research.”

Large business

“I don't think news stories [on cyber attacks] have any impact on a day-to-day basis because not every company is being hacked and is subject to cyber attacks all the time. It's like general crime, you don't think about it. It's not you, is it.” **Medium business**

"We just trust them. They have been in business for a long time. They run huge events. They are world-renowned and respected. We have faith-based on that."

Microbusiness (in UK companies between 0 to 9 employees) (Rosling, 2021)

These comments show that no one likes to spend on Cyber Security. The feeling is of someone who needs to pay a security guard to walk on the street. Executives do not have real involvement, and the micro-business is having blind faith in vendors of Cyber Security. They have no option and are moved by fear. It is a legal business, but micro and small business have no choice and is very fragile in this Cyber Security.

In Table 3 it is possible to see how much money the UK spent on Cyber Security. Micro and small businesses spent money with much more difficulty.

Table 3 Average investment in Cyber Security in the last financial year (UK). Source (Department for Digital, 2019)

	All businesses	Micro/ small businesses	Medium businesses	Large businesses

Mean Spend	£5,100	£3,490	£25,100	£277,000
Median Spend	£200	£200	£5,000	£42,600
% spending £0	33%	33%	18%	16%
Base	1,272	933	204	135

One critical question in this survey (Department for Digital, 2019) is: How much do you agree or disagree with the following statement? Do the people dealing with Cyber Security in organisations have the right Cyber Security skills and knowledge to do this job effectively? Answered: 46% Strongly agree 31% Tend to agree.

The same survey (Department for Digital, 2019) asked: Who is responsible for Cyber Security? Medium and large firms have specialist staff dealing with Cyber Security. It indicates that most companies do not have access to Cyber Security specialists. It is relevant in this research. When IT professionals are more capacitated in general Cyber Security skills, these micro and small companies will have more security.

In 2019, 40% of small companies and 28% of Microbusiness had experienced Cyber Security breaches in the UK according to (Statista.com, 2020). For 61% of large companies had to, but this kind of company has the best teams, the best software, and the best equipment that money can pay. Microbusiness just has faith.

According to (Acunetix, 2019) 87% of websites having medium-security vulnerabilities, among 46% having serious vulnerabilities.

The skill gap is a UK problem according to the UK Government (UK Department for Digital, Culture, Media & Sport, 2020), see below some data from this report.

- Around 653,000 businesses (48%) have a fundamental skills gap. The most common of these skills holes are configuration, storing or custody personal data, and detecting and removing malware.

- 30% have more advanced skills gaps;

These gaps are also common in Cyber Security companies. It extends to both technical and non-technical skills, being that technical skills gaps are relatively high in areas like threat assessment or information risk management; assurance, testing; Cyber Security research and implementing secure systems (UK Department for Digital, Culture, Media & Sport, 2020).

If the number of new Cyber Security specialists growing each year (Wang, et al., 2019), why the number of threats is so significant, and the number of vulnerabilities is too high, and companies feel that they do not have sufficient Cyber Security skills in their companies?

Society is certainly doing something inefficiently. This research aims to demonstrate that the format chosen by society to educate IT professionals must be changed. Society is creating more and more Cyber Security experts to save us from the problems that the same society still creating.

Using a straightforward analogy that everyone knows, residential waste. Imagine that people stop teaching children that they must properly handle and dispose of household waste and start investing all society's effort in training and hiring professional and specialized street sweepers. Drawing a parallel with Cyber Security is what society is doing when Universities let IT professionals trained in Computer Science receive their degrees without basic Cyber Security training (Ruiz, 2019).

Studies about Cyber Security education, normally are to improve quality into

Cyber Security specialized undergraduate courses and not to introducing Cyber Security into regular computer science courses (Bishop, 2000). Computer security includes analysing a situation to figure out what constitutes security, specify requirements, and design a system to implement the system or program correctly (Bishop, 1997). Clarification on cybersecurity must be provided from childhood according to (Sharipova & Khudayarovich, 2021)

“Undergraduates who wish to study computer security are generally relegated to graduate courses or independent study courses. Very few undergraduate computer security courses are taught now.” (Bishop, 1997). It is a scarce reference in opposition to a wave of specialization mentioned also by (Zatko, 2016) (Taylor, 2006) (Bishop & Elliott, 2011). Finland understands cybersecurity as critical and invests its efforts in training more specialists (Martti Lehto, 2020).

The late and optional security education for computer science students causes many students to graduate without any Cyber Security base or knowledge. *“The “security as an afterthought” mindset is a natural consequence of the way in which security is taught.”* (Zatko, 2016)

Other authors discussed Cyber Security education in graduation courses, again discussing specialization (Taylor, 2006).

A critical discussion is provided by (Bishop & Elliott, 2011) when trace relations with “secure programming” and “security” to propose more robust software.

According to (Taylor, 2013) students who learn about secure programming are myths and this research disagrees. Taylor’s paper has three references in two pages and does this affirmation based on personal experience or feelings. No studies that can measure the results of secure programming education was identified. But certainly, by

analogy with other areas and studies, it is possible to say that education always produces beneficial effects and support that teaching early is the best manner for brain absorbed knowledge. (Bloom, 1956)

“Myth #2. If students learn to write secure programs, the state of software and system security will dramatically improve. Programs rely on an operating system, library, and other services. Further, system security relies on systems being set up and configured as required for the particular environment in which the system is used; the size of the gap between this and practice is unknown but probably large. Companies must also provide support for the use of these skills. Whether organizations that develop software and systems will be willing to pay this price in practice is unclear, as is whether customers will be willing to pay higher prices, and endure longer development times.” (Taylor, 2013)

This study completely disagrees with (Taylor, 2013). Teaching more, better, and at the right time about Cyber Security may not be the solution to all problems according to the experiences verified in other studies (Bloom, 1956) (Bishop & al., 2019) (Schneider, 2013) and each individual's life point to the great importance of teaching more, better, and at the right time.

“Designing robust and secure systems is of paramount importance to protect digital assets and limit the attack surface available to the adversary.” (Modesti, 2020)

For (Bishop & al., 2019) the lack of basic teachings about Cyber Security in the curriculum and the almost complete absence of advanced instructions makes the student feel that he should not attach any importance to security. In the same work about robust tech programming, the authors said: *“it is clear that the effect of the secure programming clinic on students”* (Bishop & al., 2019).

A six-year kid does not need to be a master chef, but parents need to teach early about staying safe close to the stove. It is common sense. Why is it so different about teaching Cyber Security? *“An educated workforce is essential to building trustworthy systems”* (Schneider, 2013).

Researches exist in the opposite way to include more social sciences content into specialized Cyber Security courses (Kessler & Ramsay, s.d.) (Ghemri & Bouras, 2018) (Zoto, et al., 2018). If the European Commission says that members need to increase awareness of citizens and businesses on Cyber Security issues, it does not make sense that computer science students have a low Cyber Security education level (European, 2017). Also in India, Cyber Security education is not part of the undergraduate curriculum. (Joshi, et al., 2012)

Cyber Security is so relevant that it is how ALL software should be developed. *“It should be taught in almost every course in a computer science curriculum because Cyber Security affects every major software component in any computing system.”* (Lodgher, et al., 2008)

2.1. Literature review about Privacy

In Chapter 4, privacy issues will be discussed, and these four elements will be intrinsic and present, Technology, Environment, Process and Social aspects.

Currently, privacy concerns have gained an important place in people's lives; however, behaviour concerning privacy is different. (Dienlin & Trepte, 2014) Discusses in depth the privacy concerns that people have and actions relating to privacy that are adopted.

According to (Sadok & Bednar, 2015) (Maclean, 2011) (Cebula & R.Young, 2010), the massive focus of technical aspects is one of the reasons for deficiencies of

Cyber Security, and systems are composed of people, processes, and technology. Users are more and more concerned about confidentiality and privacy in web-related operations, presses companies to present more secure solutions that respect the right to individual privacy, including regulations in some countries. Conceptually, trust is the firm belief that one has concerning another person or a company. Several security incidents start in the confidence that software and hardware would not fail under certain conditions. However, as some sources show, the most common browsers on the market cannot maintain adequate privacy, even with the adoption of *InPrivate* or *incognito* browsing mode (Ruiz, et al., 2012) (Ruiz, et al., 2014) (Ruiz, et al., 2015).

It is an opportunity for law enforcement agents and criminals too.

“...security practices and strategies have not adequately kept up with dynamic and challenging attacks that are highly complex and difficult to detect.” (Sadok & Bednar, 2015).

“The protagonist of technology in data leakage and loss of privacy is evident, but Technology is not the only responsible for data leakage.” (Sadok & Bednar, 2015) (Delamaro, et al., 2007). Users are influenced by marketing campaigns that reaffirms the quality of products and services. This work explores the design structure and old vulnerabilities, which are still present in recent software that allows data leakage and privacy loss in a general way. The humans behind creating the software are responsible for the process, environment, and technical elements that cause these vulnerabilities.

Browsers are the platform for E-banking systems and other financial applications providing service. Even though in some cases new security features such as the use of tokens increase security levels, this research still keeps checking that browsers and many e-banking systems fail to provide the requisite confidentiality level

(Ruiz, et al., 2017). During the last ten years, this research improved the methods to identify on the vendor manual how the software works and verify if it fulfils what the vendor promises using conventional and unconventional system tests and reviews of security best practices. Blind faith in the promises of vendors can be dangerous for all society.

The relevance of software testing is to show the defects if they exist (Delamaro, et al., 2007) and according to (Barabanov, et al., 2018) the test of software can clarify if it does what it proposes to do. This work is to identify possible weaknesses in browsers that can compromise the privacy of customers. The Quality of Software in terms of security, it leaves something to be desired. The cause of this perception of low quality may be in software development professionals' training model. In Private Web Navigation, the first point investigated in this research tested traces of navigation using virtual machines (Ruiz, et al., 2012), (AGGARVAL, et al., 2010). Started general questions about real privacy in the private mode navigation but having no success to find local storage (Ruiz, et al., 2014) (Ruiz, et al., 2015). Bringing more and more elements that compromise the “in private” (Microsoft, 2014) or “*incognito*” mode. Tests were performed in Windows 10 Virtual Machines and Bare Metal Hardware. Four different sets of actions were tested on the browsers (Opera, TOR, IE, Safari, Chrome, FireFox and Edge) at the standard guest virtual machine Virtual Box (Ruiz, et al., 2014) (Ruiz, et al., 2012) (Ruiz, et al., 2015). The results were to be analysed and structured to show how it was possible to recover full HTML pages and images.

In all four types of tests performed in the browsers: shutdown, freeze, kill the process and power-down (Ruiz, et al., 2015) (Ruiz, et al., 2012) (Ruiz, et al., 2014), is verified that all browsers tested presented flaws in their private browsing feature. Those issues allow the identification of pages visited and, in some cases, to partially

or rebuild them.

“Security is a feeling of protection, necessary and indispensable to society and each of its members, against threats of any kind”. The defence is a capable action to sustain security feeling (Escola Superior de Guerra, 2013).

Aggarwal et al. (Aggarwal, et al., 2010), establishes an attack model between site attackers and web attackers. Also, the study is based on a technique where they discoverer how to remotely test if a browser is in private browsing mode. They describe the deepest analysis was conducted in Firefox 3.5.

In (Mahendrakar, et al., 2010) the tests were performed to do some standard tests. They analysed the existing content in virtual memory after using the browsers Firefox, Internet Explorer, Chrome, and Safari in virtual machines.

Now (Chivers, 2014) presents an Internet Explorer 10 study, especially about *InPrivate* Browsing. The author pointed out that Internet Explorer showed in Windows 8 marked a shift in how internet history and cache memory data are stored within the file system. The system was replaced with a high-performance database technology known as the Extensible Storage Engine (ESE). The prospect of recovery of evidence, together with its potential forensic relevance, raises ask. Where and when such evidence can be retrieved?

In (Ohana & Shashidhar, 2013), Internet Explorer 8 among other browsers are studied and relate residual artefacts from private and portable web browsing sessions and their tests were conducted based on Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome, but they used Microsoft Windows 7 Professional 64 bits.

Analysis of private browsing functionality by (Aggarwal, et al., 2010), lists the

profiles of probable aggressors, models of security to be checked and the goals to be met by private browsing implementations.

Privacy is important; any element related to the resources used may be the key for leaking data. All browser plugin must be compliant with the security policies in use:

“Browser plug-ins and extensions add considerable complexity to private browsing. Even if a browser adequately implements private browsing, an extension can completely undermine its privacy guarantees” (Aggarwal, et al., 2010).

The attackers may be local or remote. Locals attackers have physical access to the user’s machine while the second one can only launch attacks through network connections. According to (Aggarwal, et al., 2010) is possible to classify the changes caused by the user’s navigation actions in four different categories:

- Changes caused by web site independent of the user actions, e.g. caching;
- Changes caused by Web site but dependent on the user actions, e.g. adding a certificate;
- Changes caused directly by user actions, e.g. adding data to a form field;
- Changes are caused by other sources, e.g. updating the browser;
- Changes in any category could be the source of a breach of private browsing.

This work starts from the methodological framework presented by (Aggarwal, et al., 2010), constructing the following methodological model: Assuming that attacker

has local access to the user machine. Attempts to circumvent the system of private browsing will occur from an image taken from the machine's hard drive.

As the focus of the evaluation is the private browsing feature, considering that the user does not adopt other security tools or techniques that can cause some influence in navigation as an example of such influence, (Casey & Stellatos, 2008) considers the impacts on forensic evaluation caused by the adoption of cryptographic methods. Given the circumstances, (Casey & Stellatos, 2008) points out that forensic analysts should consider performing live system forensic, when possible, in systems where FDE (Full Disk Encryption) is applied.

Forensic analysis of browsers: One can consider the specific objects such as files and data structures or characteristics of each of them or execute a browser-separable forensic examination of the entire file system searching for important data.

In (Oh, et al., 2011) are proposed a new tool for forensic analysis in the browser presenting a list of browser structures, such as history, cookies, download lists, bookmarks, cache, and index.dat file that could be targeted. Also, they propose a method to get a record of search engines used in the browsers using signatures.

This research focuses on searching the fragments of data from which images or text that brings information about visited pages can be restored. The specific analysis of files used by browsers such as history, cookies, cache, and certificates were not considered. This analysis of those characteristics can be found in (Aggarwal, et al., 2010), (Oh, et al., 2011), and (Mahendrakar, et al., 2010).

Today, many schools and universities recommend using private browsing in their labs (University of Michigan, 2018) (Wake Forest University School of Business, 2018). The use of the private mode gives a false sense of security, leaving people even

more vulnerable.

Non-technical issues often increase the lack of Information security. Certainly, several security incidents start in the excessive confidence that software and hardware would not fail.

The social process of confidence turns security breaches in the private mode function of browsers a severe problem. Logically, the information provided by the developer is considered usually not questioned or simply accepted as true.

- Can privacy be guaranteed when the browsers are used “*InPrivate* mode” or “*incognito* mode”?

As mentioned earlier, trust is a social process that may, at some point, be abused.

From this concept, this work can derive issues on technology, process quality, environments and people that need to protect sensitive information. The complexity and connectivity of critical infrastructure systems grow; the risk of Cyber Security fails.

Relevant aspects of protecting secrets include cryptography algorithms, software applications, and Attitude. Cryptography algorithms - The algorithms are based on math and expend much effort to be attacked. Advanced Encryption Standard (AES) is an example of cryptography algorithms. Software Application – Software allows users to use various algorithms. Samples of software are Symantec Encryption Desktop (SED), Truecrypt, Veracrypt, Ciphershed, Microsoft Bitlocker, and Bitdefender Total Security 2015 File Encryption. Attitude – Individuals want to guarantee confidentiality, integrity, and availability. On the other hand, they are responsible for their actions, and they must follow the security policies not to weaken the information security. A survey conducted by Insight Express and Cisco (CISCO,

2014) keen out what Information professionals observe about corporations' data loss incidents and reply why entities need to protect society secrets:

“70% of IT professionals believe unauthorized programs resulted in as many as half of their companies ‘data loss incidents.’” (CISCO, 2014)

“44% of employees share work devices with others without supervision” (CISCO, 2014)

“39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company’s network or facility.” (CISCO, 2014)

“46% of employees admitted to transferring files between work and personal computers when working from home.” (CISCO, 2014)

“18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy”. (CISCO, 2014)

Furthermore, creators often exaggerate with promises ensuring highly efficient protection, perhaps outside real security. Underneath certain conditions, this assurance can hide threats. Some faults are difficult to detect, such as enabling revoked users in cryptosystems.

“Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA- National Aeronautics and Space Administration and research laboratories.” (The New York Times, 2005). Forbes Magazine report that NASA Hit By 366% Rise In Cybersecurity Incidents After Budget Cuts (Chandler, 2020). Also (Kovacs, 2021) report in 2021 that NASA identify over than 6000 cyber incidents in past four years.

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the

most widespread and critical errors that can lead to severe software vulnerabilities (Christey, 2011). Frequently permit attackers to completely take software control, steal data, or prejudice the correct software work. This work focus to explore Incorrect Authorization and Authorization Bypass Through User-Controlled Key - CWE 639 (Christey, 2011).

Both agencies and governments are difficulties with such infiltration. Crook groups are allocating their representatives in strategic positions for the motive of illicitly acquiring valuable interior information. Criminals pass so far as to sponsor people in their research to fulfil this aim (G1, 2013).

2.2. Literature review about Encryption

A survey by the Ponemon institute presents alarming records on the harm brought about to companies (Ponemon Institut, 2014). The theft of a pc can value as much as \$USD115.000 in credibility or public image (Ponemon Institut, 2014). The same survey suggests that the encryption notably reduces the robbery's profit: while the theft of a system with unencrypted HD fees \$USD 56,165, one that becomes encrypted loses its value on the black market. (Moreira, 2009).

A document in Computerworld mag's internet site has attracted attention by citing actual instances of its specialists thoroughly placed in huge and authentic agencies, using their positions of belief to dedicate crimes. This record also affords studies, which suggests that one in three it; specialists' secret agent systems of the organization and his colleagues, accessing statistics inclusive of contracts, wages, emails, and other strategic data. (COMPUTERWORLD, 2007).

Encrypting documents is a need and used since the Ancient Greeks and has been widely used by all armies since the beginning of the great civilizations and

certainly since the first children who wanted to communicate without their parents' interference.

A constant concern to increase the complexity of encryption algorithms has been motivating researchers and the industry ever since; a historically recent example that has affected people lifestyles until today was the enigmatic machine's ingenuity, widely used in the Second World War by the Nazis.

Cryptography is an area studied as a two-way road. If, on the one hand, more and more efficiency is sought to protect the information, the same intent of resources is used in the study of breaking these codes because the opponent also hides his information in an endless battle.

Enigma's base code had already been broken by three Polish researchers (Baker, 2018) Marian Rejewski (NSA, 2014), Jerzy Różycki (Tytus, s.d.) and Henryk Zygalski (Tytus, s.d.) as early as 1933 and served as the basis for Alan Turing's studies.

As important as mathematics, it was espionage techniques (DW, 2015) and the human factor that helped overcome the Nazi Enigma. This work follows this line of reasoning in the quest to overcome modern cryptographic programs, leaving mathematics to mathematicians. This study uses software implementation failures and characteristics of human behaviour to gain access to information protected by cryptography. This work looks for methods and techniques to bypass de key and does not intend to break the cryptographic algorithm explained by (KNUDSEN, 1999). Other's author describes a variety of attack scenarios.

In (Thomas, 2003) he classifies the possible attack attempts based on the data that an attacker can procure: Ciphertext-only attack; Know plaintext attack; Adaptively chosen-plaintext attack; Chosen ciphertext attacks, also (Thomas, 2003) divides

possible attacks into two categories: Practical attacks and Theoretical attacks, that focus on the mathematical aspects of the chosen cypher algorithms. Besides (Thomas, 2003) presents the attack tree, a structure that describes system security using different attack possibilities as parameters.

Under (KNUDSEN, 1999) and (Thomas, 2003) classification system, proposed attack 1.3 would be ciphertext-only and practical instead of theoretical. This work methodology is based on this attack type.

To (GALLIANO, 1979), P.6, the method is the "*set of steps, neatly arranged, to be overcome in the search for truth, in the study of a science or to achieve a particular purpose*".

According to (Barabanov, et al., 2018) and (Delamaro, et al., 2007), software testing is to show the presence of defects if they exist

As the focus is to evaluate the functionality of password protection of a Truecrypt container, other aspects such as the type of encryption used and the use of full-disk encryption protection of the disk will not be addressed in this work.

When the trainee configures the Truecrypt or similar software to an executive, politician, general, or researcher, installing the software with the password "123" all of these persons are inducted to change the password and type a "Strong Password". This procedure is standard and puts the power of billions of dollars in the hands of the trainee (IT Services, The University of Manchester,, 2014) (University of Exeter, 2014) (Wake Forest University, 2014). The way to gain access to the new data with the old password is to change values in the reader of the container file mixing old and new files. (Ruiz, et al., 2014)

A large Brazilian oil company reported that the theft of equipment containing

sensitive information about the discovery of new oil wells affected the value of its shares negotiated on the stock market (G1, 2013).

Studding Software testing (E. DENNING, 1987) declares that major systems have vulnerabilities. In the Chapter 5 the contributions in this field will be presented.

2.3. Literature review about Web Credentials

The function of credentials, according to (Smith, et al., 2020) is “to certify the identity and the institutional status (including certain rights) of individuals”. In a very extensive a complex environment, it is a natural unsafe place to do anything. Play in this place needs to observe the entire environment and all parts need to check all safety rules to turn it more usable. Blind faith is not a choice.

On the internet, exists a large number of malware made to get user credentials like (Kuraku & Kalla, 2020), normally banking malware is not generic and is made for each bank and country. This fact turns more relevant to each bank's responsibility to improve the best code and practices to develop their home banking sites.

“The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives”. (Sadok & Bednar, 2015).

In discussing authentication problems, (FU, 2001) presents three categories of attack in the first one, called existential forgery, an attacker can forge an authenticator for some unspecified user, which means that he cannot target one specific user. In the second class, called selective forgery, a specific user can be targeted. In the third and final class, called a total break, an attacker can recover the user key and is, therefore, able to build valid authenticators at will. The research discussed herein points to the existence and importance of attacks targeting authentication data. Also, (OH, 2011)

analyses a vast class of information about the navigation activities that browsers save to disk.

Incessant assessment of operating systems, browsers and cryptographic programs have disclosed many failures on cookies and history files of web browsers (AGGARVAL, et al., 2010) and (CARRIER, 2005).

"A taxonomy also allows for previous knowledge to be applied to new attacks as well as providing a structured way to view such attacks." (HANSMAN, 2004). About it (LOUGH, 2001) presents a taxonomy of computer attacks named VERDICT acronyms to Verification, Exposure, Randomness, and Deallocation and in the same work proposes a new taxonomy based on dimensions:

The base dimension is applied to categorize the attack based on its vector or closest class if there is no specific vector. The second dimension is applied to categorize the attack based on its target. The third dimension is applied to categorize the attack based on the vulnerabilities and exploits. The fourth dimension is applied to categorize the attack based on payloads and secondary effects. Episodes can focus on information acquisition for further attacks.

Also, inside the third dimension, (HOWARD, 1997) presents password vulnerabilities categories and in the same topic, (HOWARD, 2010) presents the vulnerability called *"Failure to protect stored data"*, (SEACORD, 2005) presents the CERT taxonomy for user interface and others implementations vulnerabilities. While (SOOD, 2006) explores malware taxonomy.

About cookies (KHU-SMITH, 2002) describes Malicious application deployment through cookies. Confidentiality of data stored and monitoring user's browsing habits through cookies.

Discussing authentication issues (FU, 2001) shows three categories that an attacker could achieve. In the first one, called existential forgery, an attacker can forge an authenticator for some unspecified user, which means that he cannot target one specific user. In the second class, called selective forgery, a specific user can be targeted, Besides, (OH, 2011) analyses navigation activities that browsers on non-volatile memory.

This chapter is focused on Client-side credential management. Diverse from presented in (OH, 2011), this work focus only on the analysis of authentication data found on a hard disk.

Data carving is the principle used by this study to deep dive for bypass banking credential management systems and data carving can be generalized as:

“By using a database of headers and footers (essentially, strings of bytes at predictable offsets) for specific file types, file carvers can retrieve files from raw disk images, regardless of the type of file system on the disk image.” (RICHARD III, 2005)
“...open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools.” (CARRIER, 2002)

To (Nelson & Jeske, 2013) a third part software helping web browsers to encrypt data is a solution to protect bank transactions on WEB, however, in Brazil, a similar method was used by Caixa Econômica Federal (Caixa Econômica Federal, s.d.), a Brazilian bank that use a third party software to protect bank transactions on the web. This study bypassed this system because while the system was concerned with strongly encrypting the key transmitted over the web, it forgot that the browser recorded the key in clear text on the victim's computer. New tests are conducted in 2020 and the results are the same.

While works like this thesis point out flaws and look for a common source of software quality problems and propose a general solution to increase security, other works attack the effects like an acetylsalicylic acid acting on the impact turning more and more difficult for users to get access to bank account and other services. In some cases, banks request the user to have a cell phone to run an app to provide temporary codes and memorize three different passwords (Boonkrong, 2017).

When looking for WEB credentials, most studies are focused on how browsers store users and passwords for the sites where these users browse. It is necessary to make it clear that the research that this thesis is about has nothing to do with this specific and widely studied situation.

While authors (Ahmad, et al., 2015) compile studies towards the standard password storage provided and consciously managed by browsers, this thesis is based on the unknown and unconscious storage produced as a waste of processes poorly conceived by the programmers of the operating system, browser, and the page visited.

2.4. Literature review about Security Systems

"Viruses are the most abundant parasites on Earth" (National Science Foundation, 2011) and to Cohen that defined "computer virus," it is very similar to a biological virus. The infection process and the comparison with the similarity with biological systems is part of (Filiol, 2005) work that made this deep characterization. *"Computer Viruses, Artificial Life and Evolution"* is a book that describes the possibility that computers can simulate life or an artificial life (Ludwig, 1993). Also (Ludwig, 1995) introduce the best approach and opens the door to Darwinian evolution to a computer virus. For (Gould, et al., 2020) is necessary to trace a parallel with algorithms and biology to the evolution of Cyber Security.

The treats are faster than protection (Ford, 2004) *“While the antivirus industry has been steadily improving over the years, it may come as a surprise for some to realize that the fundamental technology used for detecting and removing viruses has changed very little over time”*.

To (Department Homeland Security, 2009), pp.38 *“Malware refers to a broad class of attack software or hardware that is loaded on machines, typically without the knowledge of the legitimate owner, that compromises the machine to the benefit of an adversary”*

Misuse detection is based on signatures (Mohsen Damshenas, 2013), (Farid Daryabar, 2011), and 100,000 new malware were catalogued every day in 2013 (McAfee Company, 2013), the concept of signature is questionable as possible to see in the section 3.3.1. Many samples of massive damages are in the new. Stuxnet (Weinberger, 2011) (Langner, 2013), I Love You, and many others like a virus that erased data on three-quarters of Saudi Aramco computers (Lasiello, 2015).

In (Tadmor, et al., 2011) statistically reduce detection when the virus was specifically associated with the host, linking the host, injecting its DNA into the host, and embodying into the host as a prophage (a viral genome inserted and integrated into the DNA of bacteria).

(Parry, 2012) used a virus called "Lambda", which performs extremely quick changes, and can infect a bacterium through a new door. Normally, the lambda virus is capable of infecting E. coli cells. This research was inspired by biological research of (Zhao, et al., 1998), (Tadmor, et al., 2011), and (Parry, 2012) that inspired the tests to explore the antivirus systems.

Security is a protection feeling (Escola Superior de Guerra, 2014). Based on

the concept; questions may be derived to address information technology and software so necessary to environments and systems that need quality and efficiency to safeguard critical information. Cyber threats exploit the increasing complexity and connectivity of essential systems of infrastructure, putting security at risk. In the context of cyber threats, malware is trending in various productive sectors. According to the company's report (Check Point Software Technologies Ltd, 2014), almost 84% of the organizations surveyed were infected with malware. According to estimates by (Check Point Software Technologies Ltd, 2014) experts, 2.2 unknown malware hits companies once every hour. An anti-malware system gains special importance because it represents the last element of defence before an attack is consummated, and the cyber virus is similar to biological systems (Filiol, 2005) (Ludwig, 1993) (Ludwig, 1995)

(Nissim, et al., 2014) provides a method to improve detection while the nature of technology changes quickly, equally, the nature of malware. The various anti-malware software manufacturers announce new and efficient technologies that aim to provide better performance and cheaper responses in malware security incidents within organizations.

Similarly, the purpose of anti-malware software testing is to identify possible weaknesses in systems and assign values with key performance indicators that allow classifying systems appropriately through these attributes. The version of the Brazil Method was presented at the Symposium on Operational Applications in Defence Areas.

Magazines that are sponsored by the same companies that they evaluate provide tests of antimalware systems. Which is an obvious conflict of interest: VB100 (Virus Bulletin, 2014); AV-Comparatives (AV COMPARATIVES, 2014); Anti-

malware Test (Anti-Malware-Test.com, 2012); AV-TEST (AV Test, 2014); ICSA Lab (ICSA Labs, 2014); NSS Labs (NSS Labs, 2018); West Coast Labs (West Coast Labs, 2014) and EICAR (EUROPEAN EXPERT GROUP FOR IT-SECURITY, 2020). This kind of relation is partial and not recommended to serve as the base of public purchases. (FLEISHMAN, 2018) (Consumer Watch, 2015) (Hachman, s.d.)

A theoretical model is presented in 2018, four years after Brazil Method by (Nurhayati, et al., 2018), but without real tests having been carried out. Other test methods are published after Brazil Method (Bai, et al., 2019), (Valdi, et al., 2015), and (Shevchenko, et al., 2019).

2.5. Literature review about Cyber Security

Education

People are always at the centre of problems caused by Processes, Technology, or the Environment. People create Processes, Technology, and Environment to give something to people. We, the people, are in the centre of all. To (Dawson, 2017), is necessary to understand the requirements for the national and regional or accredited Cyber Security programs. For the first time, Cyber Security is at the top of threats second (World Economic Forum, 2018).

“From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human process rather than entertaining an expectation of a one-sided change of behaviour of the end-user.” (Sadok & Bednar, 2015).

If all Cyber Security problems derive from people, it is clear that people are not learning correctly. The National Security Agency (NSA) provides Cyber Security courses accreditation in the scope of the National Initiative for Cyber Security

Education (NICE) Framework (Shoemaker, et al., 2016). But this covers just Cyber Security specialist courses.

There were 79,480 students enrolled in Computer Science courses in the UK in 2016/17, according to (HESA, 2018). This study analyses the G400 courses discarding any specialized Cyber Security courses. Intending to that is necessary to form computer science people that know, respect, and use Cyber Security in the base of any software and environment.

What is expect about Cyber Security and privacy when Universities teach a user to share their credentials? See below some examples of it:

"We use TrueCrypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume password or pre-boot authentication password when a user forgets it (or loses a key file)? Yes. Note that there is no "back door" implemented in TrueCrypt. However, there is a way to "reset" volume passwords/key files and pre-boot authentication passwords" (Wake Forest University, 2014)

"If necessary, eg when someone who knows the password leaves the University, you should choose a new password (using the guidelines for choosing a strong password) and then contact us for advice on how to change the password". (University of Exeter, 2014)

"If someone needs to access an encrypted file or a shared encrypted laptop, the encryption password will need to be shared, unlike your University password which should always be kept private. If you forget the encryption password for a file or USB stick, then the data will be inaccessible. In the case of laptops encrypted by the University, IT Services will store a recovery disk that will enable the laptop password to be reset." (IT Services, The University of Manchester,, 2014)

In the same line, when Universities orient their user to use "in private" navigation that this research explains in the chapter about Privacy, is necessary to stop and review what is teaching about security and privacy. (University of Michigan, 2018) (Wake Forest University School of Business, 2018)

“...two reasons could potentially explain the poor effectiveness of the implemented security solutions and procedures: the boundary problem of risk analysis scope and the background of involved actors in risk assessment and security policy design.”
(Sadok & Bednar, 2015)

Austria, Australia, Finland, France, Germany, Ireland, Italy, Japan, Lithuania, Portugal, Republic of Korea, South Africa and Spain intend to include Computer Science in secondary education as compulsory (Passey, 2017).

According to (Ferrari, 2013) The European Commission proposed that each student know Cyber Security as a beginner, intermediate and advanced in progressive learning. This concept presupposes that or docents are prepared to do this task. It is another example that Cyber Security has been teaching as separated. This research proposes that Cyber Security needs to be part of students' daily lives. A disproportionately technical focus is one of the main reasons for the lack of Cyber Security (Sadok & Bednar, 2015).

“While information security risks have involved and financial costs of cybercrime have increased, security practices and strategies have not adequately kept up with dynamic and challenging attacks that are highly complex and difficult to detect.” (Sadok & Bednar, 2015)

To (Reza & Shareeful Islam, 2013) human factors are important and the relevance of education in information security is presented in incidents verified in financial organizations.

One-third of the pieces of software tested exhibited vulnerabilities during a two-year study, according to statistics from the Russian Information Security Certification System. (Barabanov, et al., 2018) In previous chapters, this research brings to light some of these vulnerabilities and how they can affect society.

Public, infrastructure, business, and general, according to (Ramirez, 2017) are

categories of Cyber Security. Cyber threats are present in the fundamental aspects of modern life. Introduce Cyber Security into student daily make sense. Just broadening the knowledge of security experts do not solve the issue.

“From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human process rather than entertaining an expectation of a one-sided change of behaviour of the end-user.” (Sadok & Bednar, 2015).

(Gal-Ezer, et al., 1995) declares that security is among the key aspects in the field of computing. In (Alexandron, et al., 2017) are suggested a new curriculum for teaching programming to teenagers, but without security or privacy elements.

The National Centres of Academic Excellence in Cyber Defence Education (CAE-CDE) in the United States jointly NSA are improving criteria of quality of Cyber Security education, but still focused in a specialized field (Wang, et al., 2019). New Zealand is leaving out privacy and Cyber Security in their discussions about Computer Science on the High School curricula (Bell, et al., 2010).

The UK is concerned about Computer Science teaching is to produce more programmers from the secondary level onwards (BROWN, et al., 2014) (Brown, et al., 2013) (Sentance, et al., 2012).

“The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives”. (Sadok & Bednar, 2015)

A study by (Modesti, 2020) proposes a course structure based on four pillars, Learning needs, Purpose, Activities, and Learning Outcomes:

Learning needs: As students may have varied backgrounds and prior knowledge, it is important to use the basics, assuming that everyone is at the minimum level for Cyber Security and to evolve gradually;

Purpose: It is essential to focus the relations between the students and the Cyber Security involvement for the best use of the few hours available;

Activities: Teach in practice, use labs;

Learning outcomes: Be sure to reinforce the basic principles of secure design and secure encryption, as well as concepts of privacy and the use of encryption.

Cyber Security and privacy concepts must be teaching in early education (ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, 2017), (Ruiz, 2019) and the author's contributions in this field will be presented in Chapter 8.

3. Research Methodology

This is a Prior publication thesis, and as a compendium of a large number of different publications using diverse methodology and exploring five cyber security elements.

3.1. Privacy

The concept of privacy is very new in humankind's history, and it is becoming more and more relevant the more significant the society and group where the person lives. A different culture is having other concepts of what needs to be private. This chapter intended to show how society can lose privacy and sensitive data on the internet with false vendor promises and wrong orientations. Also, this chapter explores test software issues and the relation between teaching and harmful software developed. Privacy in this work present three versions of a method to restore incognito/InPrivate mode navigation, able to expose all navigation made over incognito mode. The method

works over browsers like IE, Edge, Firefox, Safari, Chrome, Opera and TOR over Windows systems. In the next chapter a special element of cryptography is explored, the key management.

The privacy issue on the internet is challenging to solve because privacy is not about software tools. It depends on attitude change.

This change in attitude is the cornerstone to achieve the desired privacy. When seeking anonymity or privacy on the internet, the principle goes beyond the use of technological tools. People when browsing on the internet is subject to the following elements that can monitor their habits and customs: Internet service provider, LAN administrator, operating system, and other software on the computer and sites visited:

Software is always subject to failure by incorrect coding. Developers often include telemetry routines that sometimes can be sent user data to the developer without user consent. A malicious developer may use this information in an abusive manner or even sell it to interested third parties. Thus, access monitoring is a mandatory activity to establish consumer habits and geographic users' locations.

Bandits and law enforcement exploit system failures simultaneously. By user is important to verify the functionality of such a feature, if available implementations provide the degree of confidentiality promised, or if there are flaws that allow the retrieval of online activity data.

This study executes two different tests. In the first batch, four different sets of actions were performed on the browsers Internet Explorer (Microsoft, 2014), Firefox (Mozilla Contributors, 2014), Google Chrome (Google Inc., 2014) and Safari (Apple Inc., 2014).

Internet Explorer browser was tested on bare metal hardware with the use of

four notebooks equipped with Windows 7 Pro SP1.

For the other tests performed, a standard guest virtual machine was created with the operating system Windows 7 Pro - in the host operating system - Windows 7 Pro - using the virtualization software Virtual Box (Oracle, 2014).

An export (snapshot) of the newly installed Windows machine was created, considering the possible need to compare the base guest machine with guest machines running the different browsers tested.

The browsers tested were Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1 and Safari 5.1.7_1. The guest virtual machine for each browser was replicated 4 times, each to be used in the four different tests performed on each browser.

Based on those configurations, the four different sets of actions were applied for each browser in private browsing mode:

The test batch was applied one set of actions, represented by Test S, for the browsers TOR Browser Windows 3.6.6 (Tor Project, 2014) and Safari 6.0.3 (8536.28.10).

The TOR browser test was performed on a guest operating system Windows 7 Pro SP1 running over a Virtual Box (Oracle, 2014) virtual machine.

The Safari test was performed on MAC OS Mountain Lion, 10.8.3 running as a guest on a VMWare (VMware, 2014) virtual machine.

For each test performed, a clean new virtual machine with Windows 10 was created and the image generated using backup option of the virtual machine VirtualBox was analysed through the application of the program “Strings” (Die.net, 2009) found in different Linux distributions. This program was used for the search of strings inside

the virtual machine images that could present relation to the webpage visited.

The images of the virtual machines are also analysed to search graphic files associated with the visited web page through the Foremost programs (Kornblum, et al., 2002), a renowned forensic tool for extraction of files - "data carving" - of different formats.

A study about data analysis inside the Windows pagefile (Lee , et al., 2007) points out that for data extraction the two approaches represented by both tools (Strings and Foremost) have differences but are considered standard inside the forensic analysis field. About the process of file carving, one can generalize the method as:

“By using a database of headers and footers (essentially, strings of bytes at predictable offsets) for specific file types, file carvers can retrieve files from raw disk images, regardless of the type of filesystem on the disk image.” (Richard III & Roussev, 2005)

The Foremost tool works as follows: It reads a block of data - memory, disk or files - and looks for signatures (headers or footers) related to files of well-known formats. Many known problems are associated with the use of tools aiming for "data carving", for example, my cause limitations to the treatment of non-contiguous data. Thus, it is possible for an image whose sequence of bytes is dispersed to not be fully recovered, despite its possible existence in the data analysis block.

Foremost software is widely used in digital forensics. In (Vaughan, 2004) the discussion is about the use of Foremost could speed up the carving of data of XBOX executable files ("xbe" type). The WinHex tool (X-Ways Software Technology AG, 2014) was also used to search for keywords found in the navigated webpage.

Digital Forensic techniques for mobile Windows phone analysis are discussed

by (Grispos, et al., 2011) that compares the carving performance of the data carving programs Scalpel, Foremost, Simple File Carver and Phone Image Carver. Comparing file carvers (Courrejou & L. Garfinkel, 2011) chooses the following tools: Foremost, Scalpel, PhotoRec, and Adroit, concluding that the best approach is to use many tools to explore the strong points of each one.

As any forensic evidence that could potentially be used in a court of law, “...open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools.” (Carrier, 2002).

A random selection was made, aiming to simulate an actual visit to any website available on the internet, and the sites chosen for the experiment were (Discovery Channel, 2012) and (History Channel, 2014). Since some site information is proprietary, the figures recovered during the test will be only partially reproduced in the present work.

First Batch of Tests – Four Different Set of Actions as describes in Table 4.

Table 4: Test Types

Test Type	Action
S (Shutdown)	Include visiting a website available on the internet, making regular navigation to interact with the site, finishing the browser's execution correctly, and generating the virtual machine image for analysis. This test is the most favourable for both the operating system and the browser because the user follows the steps expected for the shutdown of the

	machine.
F (Freeze)	It consists of visiting a website available on the internet, making operations to interact with the site and with the browser still active, generating the virtual machine image for analysis.
K (Kill process)	Incorporate visiting a website available on the internet, making operations to interact with the site, requesting that the operating system interrupt the browser execution and generate the virtual machine image for analysis.
P (Power down)	Involve visiting a website available on the internet, making operations to interact with the site, and requesting the virtualizer to turn off the virtual machine - simulating a power outage - generating the virtual machine image for analysis.

A specific section to discuss the results is presented in section 9.1.

3.2. Encryption

3.2.1. Truecrypt

In (Ruiz, et al., 2014), (Ruiz & Winter, 2016) and (Ruiz & Winter, 2016) was demonstrated how it is possible to verify that attackers can gain full access to the encrypted files enabling revoked credentials. A wide range of cryptographic software

is tested. Truecrypt (Foundation, 2013), Veracrypt (IDRIX, 2018), Ghostcrypt (Ghostcrypt, 2018) and PGP Symantec Encryption Desktop (Symantec, n.d.).

All Truecrypt deviants provide a unique password that permits access to data by the user. The problem is that it doesn't matter how many times the user changes the password. All of them always will open the container and exposes the data.

Worldwide famous and with much acceptance among IT professionals, this open-source software is used by individuals, governmental and companies.

The development of TrueCrypt was ended in May 2014. A strange fact is that all the material of Truecrypt was excluded, including the Wayback Machine. But is still in use around the world with a lot of forks versions. Figure 4 is showing the Truecrypt screen.



Figure 4 Truecrypt screen to generate encrypted volume.

In the same way in other output (Winter & Ruiz, 2016) the method is similar to explore the case of BitLocker that was the weakening of the security system with a weaker recovery password equal regardless of the change of container password.

While the situation of Bit Defender Total Encryption 2015 is a little different. The use of misconceptions affects the security of customer information that believe in the reputation of the company. Are merged two encrypted containers and opened the resulting container with the password used in creation. This is possible because when the container was created, the original password acts as a master key for all other container versions regardless of the password change. Also, the software allows the implementation of different parts to be joined without checking the integrity of the container.

To gain access the data is needed two files; the first file is empty with password 123; this original header was saved and later merged to the TrueCrypt container after it went through the password change.

To manipulate the files is applied the following code written in Perl.

```
#!/usr/bin/perl
#cut.pl
file1 = $ $ argv [0];
$ file2 = $ ARGV [1];
$ source = $ ARGV [2];
$ size = $ ARGV [3];
open (FILE, "$ file1");
binmode FILE;
open (QRA, "> $ file2");
binmode QRA;
seek ARQ, $ origin, 1;
read ARQ, $ buffer, $ size;
QRA print $ buffer;
close (FILE);
close (QRA);

REM Extract header from D0 to H0
perl cut.pl original_file H0 0512
Resulting file: 163ed3c23f65cadab78c409ef8bb2f5b

REM Extract data from D1 to OD1
perl cut.pl file_with_data_and_new_password OD1 512
299008
Resulting file: 96e0fbef4764293681f814b1c2fb00a1
```

```
REM UNION H0 + OD1 INTO ND1
type H0> new_file_merged
type OD1 new_file_merged >>
Resulting file: 875a17624f0760af55c4e8bf89b08fec
```

3.2.2. Bitlocker and BitDefender Total

Encryption

Microsoft Bitlocker was enhanced for Windows 7 and available in Ultimate and Enterprise editions. BitLocker protects documents and passwords by encrypting the full Windows drive on where data is. When BitLocker is enabled, any file saved on the drive is encrypted automatically, according to Microsoft.

BitLocker To Go – is a feature in Windows 7, allows blocking USB flash drives and external hard drives.

Bitdefender is a Romania-based Software Company that offers the BitDefender Total Encryption 2015 to create a secure and encrypted environment according to the vendor using the logical representation of a file extension BVD (BitDefender Virtual Drive). Figure 5 shows the screen of Vile Vault creation in BitDefender.

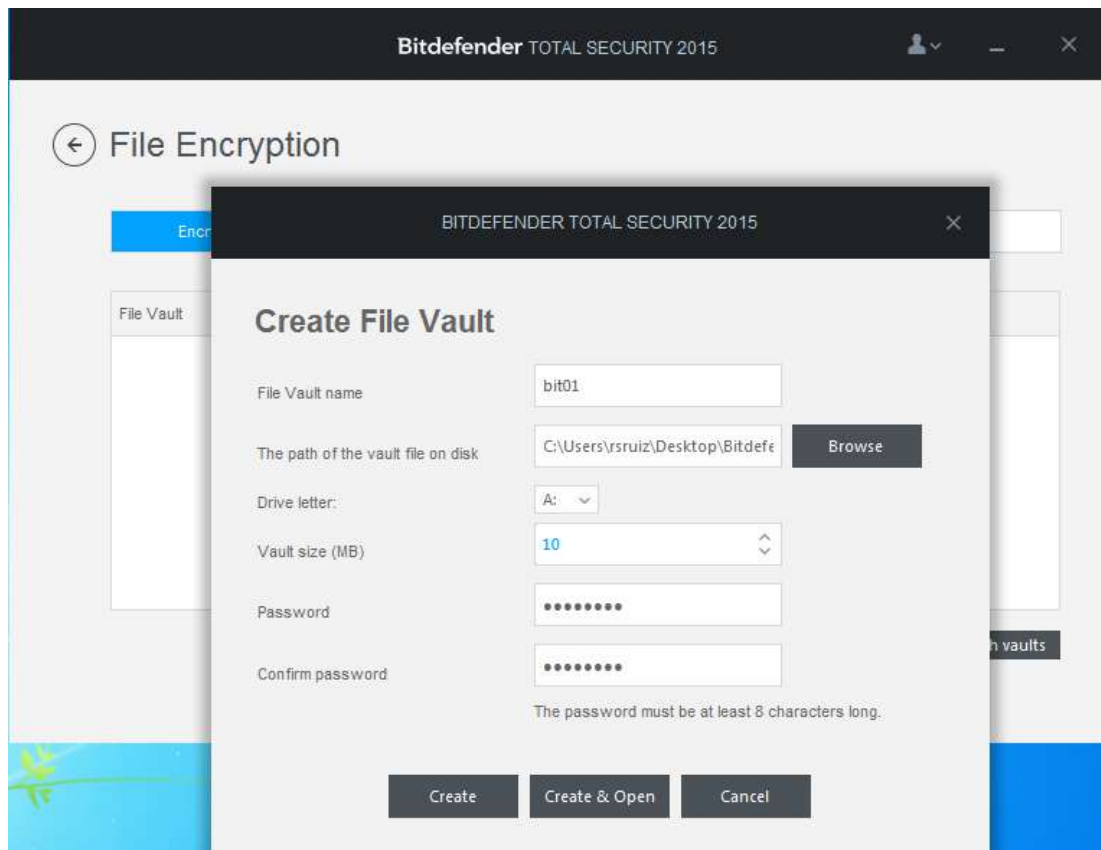


Figure 5 Bit Defender Total Encryption

Truecrypt forks and BitDefender having different designs in their files, but the same principle. Figure 6 as showing a file comparison of BitDefender 2 files. At the top, a file was created with the password 123456789 and having no files encrypted. At the bottom, the same file with data encrypted inside and a new password. Figure 7 shows the encrypted data exposed after the bypassing.

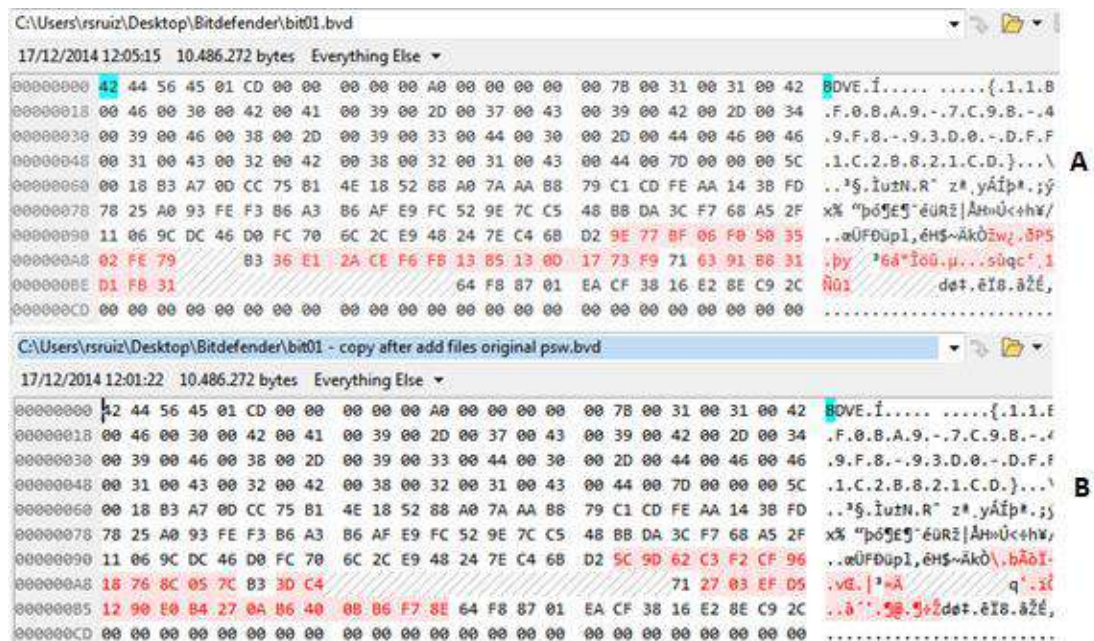


Figure 6 - BitDefender footers file comparison. In the A empty file with the password 123456789 and at B encrypted data with another password.

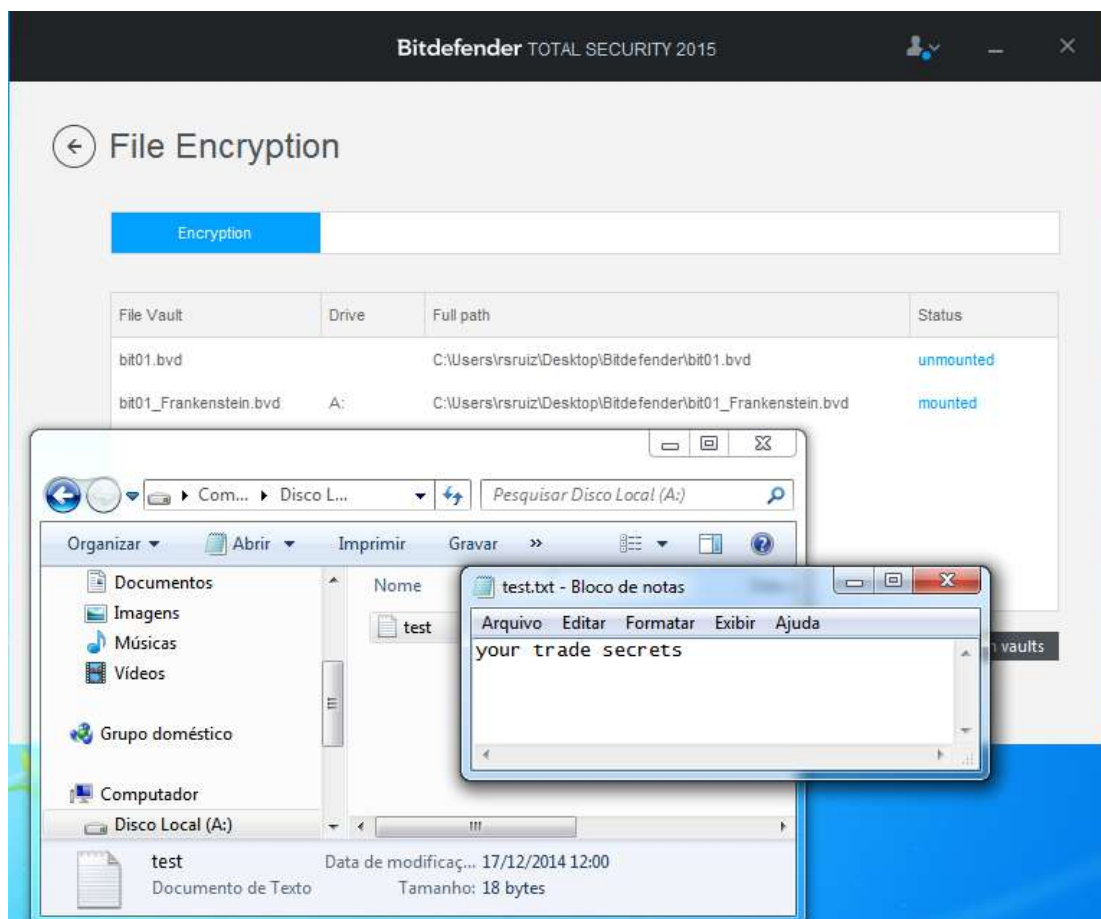


Figure 7 - The figure shows encrypted data was exposed by using the method with a deprecated password.

BitDefender Test has created a BVD(extension and format exclusive for BitDefender container files) file named. The file had its password changed to 987654321 and added a text file with sensitive information Bit02.bvd using the DitDefender. After these steps, two files with different passwords and content were available.

It was merging (using WinHex) the known password Bit01.bvd with data session Bit02.bvd file resulting in a third Bit01_Frankenstein.bvd file. As a result, it was possible to having access to the data of Bit02.bvd with the password Bit01.bvd Figure 7.

This technic permits the owner of any later release of Bit02.bvd file, and the password used in the creation of Bit01.bvd will have access to the encrypted file content.

3.2.3. PGP Symantec Encryption Desktop SED

The PGP Symantec Encryption Desktop SED (Symantec Corporation, 2015) remained chosen in this investigation for the following motives:

- The SED is founded on PGP, which is well known and has high reliability and security;
- Symantec developed SED to ease multi-user collaborative work;
- The SED creates a secure virtual encoded drive as a simple logical drive f:\ or a flash drive. Access control of this file with PGP to manage cryptographic keys is a secure protection method.

SED file has two parts: header and data unit. The header section has severe difficulties because this enables the mixing of different file versions and permit to gain access to a new file version. The reader stores all passwords for all users and it is the vulnerability exploited.

This software permits that the company creates workgroups that can access the container at the same time. Each user has a credential linked with the PGP account. An administrator can include and revoke any user. The method presented in Figure 8 and first published by author in 2016 describe how to restore and use the revoked user credentials to open a new versions of encrypted data (Ruiz & Winter, 2016). It shows a diagram Figure 8 of steps to gain access with a risen user using different versions of the container. The same paper shows all codes to reproduce this situation and propose the scenario attack. The representation of the method is presented in Figure 8 when as possible, to see the creation of Frankensfile Figure 8, reference to Marry Shelley novel, Frankenstein. With parts of an old file addicted to an actual file, it is possible to open the data with old credentials.

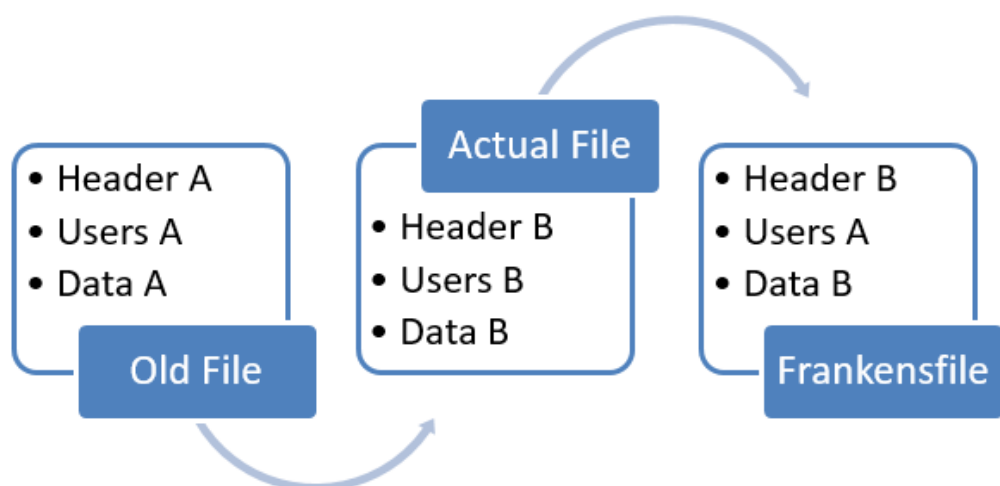


Figure 8 - Visual representation of a method to use deleted users to having access to actual encrypted data with PGP.

The method can be described as: (a) Generate PGPOrigin.pgd file and create

users (user1, user2 and user3); (b) Make a copy of PGPOrigin.pgd into PGPcopy.pgd; (c) Save the information inside the PGPsedWork1.pgd file. User1, user2; and user3 have access; (d) Delete the user3 according SED user manual (Symantec, s.d.) from PGPsedWork1.pgd file. In theory, only user1 and user2 will have access to encrypted data; (e) Make the Frankensfile.pgd file, which has the header section of PGP copy.pgd and data section from PGPOrigin.pgd.

A specific section to discuss the results is presented in section 9.2.

3.3. Security Systems

In this chapter, the side effect most directly applied to the fears of society and ordinary citizens was presented. It was explained how an attacker can obtain credentials and have access to a user bank account, make improper purchases in a third person name, have access to user emails, and recover many other accounts for access to various services. Web Credentials chapter was explored how to get clear text credentials after the analyst having access to the computer target. The proposed method can get credentials used in intranets or e-commerce, home banking and email accounts. It can be used in criminal investigations or to improve more strong security in these websites.

In more specific and targeted cases, access to specific systems of government, companies, and even the military and law enforcement can be done, generating irreparable damage for the whole of society.

A worrying fact was the attitude of the contracted companies, which mostly preferred to ignore the fact. This may be due to a standard postponement procedure for any image damage. If a bank were to suffer a similar attack, it would resort to the insurance system, reimburse the client individually by covering up the case and

avoiding the expenditure of thousands of pounds to correct the systems, train its staff and run the risk of mere vulnerability information leaking to the market. Denying costs less than to publicly admit insecurity in their structures. In Brazil and many other places, the appearance is more important than real facts. If a bank's image is tarnished by the admission of a burglary by hacking into its systems, the drop in the value of its stock on the stock exchange is several times greater than the robbery itself. In the next chapter the author explores security systems and how they can be used against the users.

3.3.1. Apoc@lypse Technique

The Apoc@lypse technique intent to demonstrate how antimalware systems can be used to improve several damages to the Operational System and it provides 3 methods of operation, T, E, and B, and each one having different effects in Operational System:

Method T - the operation is performed to replace the entire contents of the file system with any malware's DNA. Thus, as the entire file contents are replaced with a virus's DNA, any virus protection provisions of a virus signature in the database will delete the infected file.

Method B – the operation is performed to inject the beginning of a file system of the computer malware into any DNA.

Method E – the operation is performed to inject the end of a file of the computer system the DNA of any malware.

Figure 9 schematically represents the methods of injection. (T), (B) and (E). Note that in this case, the DNA virus is the EICARTM (EICAR, 1998), an inoffensive string of characters created in principle to test if the antivirus works or not. When the

antivirus finds this string in the computer, the file that contains this string was considered infected and destroyed. But that file does not harm the user's system or files. Any part of a string by any known virus can be used, and every as used just parts, no harm will be done by the DNA.

The problem occurred when the antivirus was found this DNA in the files. This causes a very serious autoimmune reaction that leads the antivirus protection system to destroy files, the system and the antivirus itself in many cases.

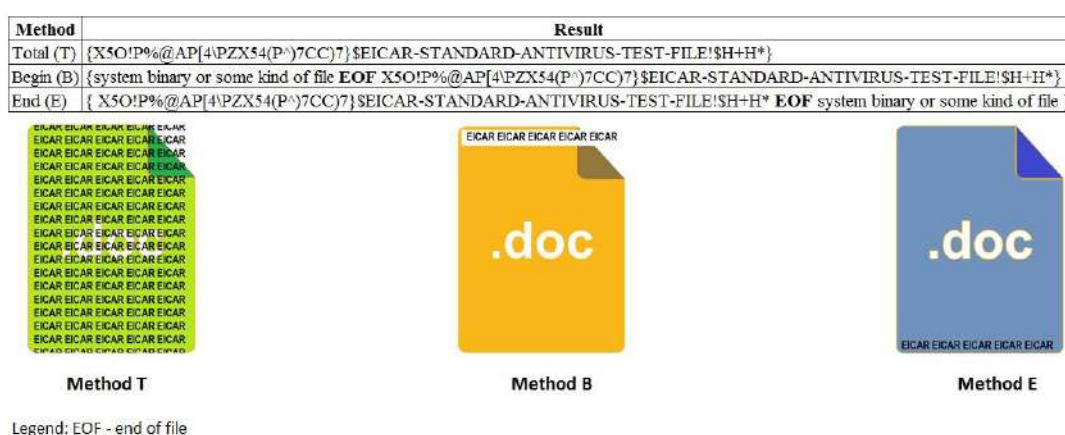


Figure 9 - Injection methods.

Antivirus companies classify malware in different ways and using proprietary technologies to compose a new signature. In this way, depending on the chosen virus DNA some antivirus will be affected and others not. Various virus DNAs were used in the tests, which, as mentioned above, were more effective in certain brands of a virus. However, a specific DNA is known as EICAR TM (EICAR, 1998) and the Apoc@lypse Technique it is possible to bypass with great success the antivirus protection and to destroy the operating system and users' data. It can be used as a military cyberweapon (Winter & Ruiz, 2016). This paper published in a British Military Magazine explores a possible scenario to use the Apoc@lypse Technique to put down the computer's opponent.

Today more than 150 antivirus software exists in the market. However, no more than a dozen nucleus core of malware detection. These dozens of vendors license their core to other interface manufacturers. (Ruiz, et al., 2015)

All of the antivirus software is affected by the Apoc@lypse technique:

“That also happened with the current antivirus software, because all of them have the common ancestors, the first antivirus software written and popularized by John McAfee and Peter Norton”
(Ruiz, et al., 2015)

The modus operandi of all old antivirus software was replicated to all current systems of anti-malware. In other words, by definition, all of the anti-malware systems work the same way in the detection and fighting off viruses and malware since the beginning.

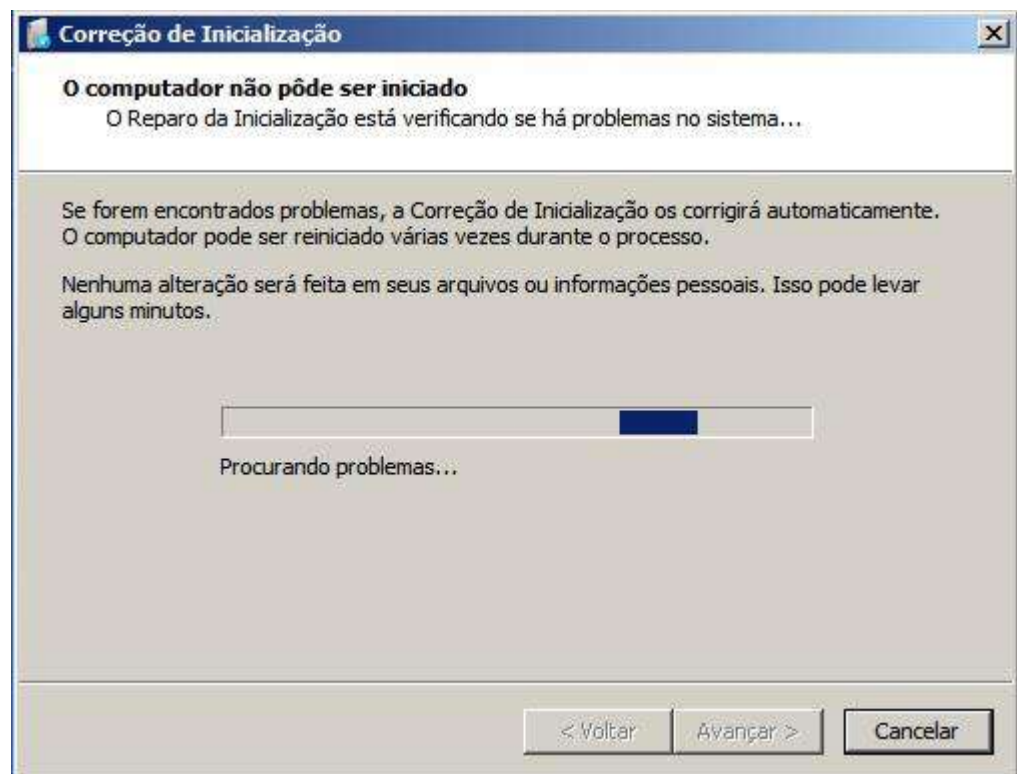


Figure 10 - In Portuguese, after Avast conclude the service " The computer can't be initialized."

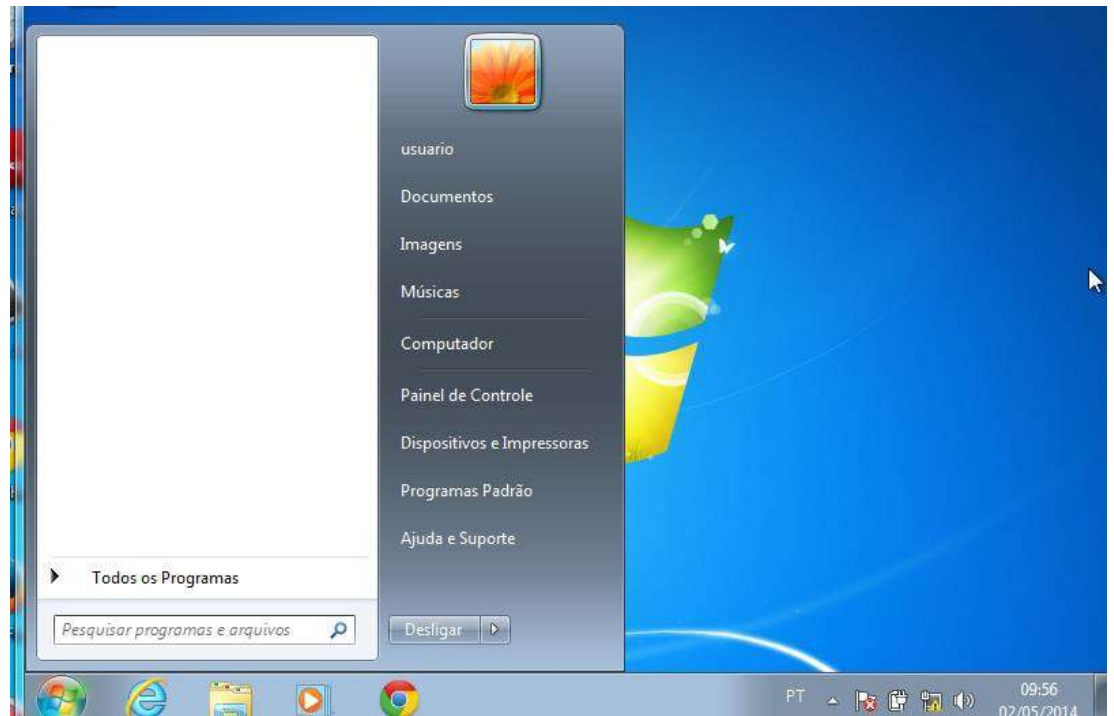


Figure 11 - In this case, Norton has destroyed all program files.

There are some similarities between the human immune system and antivirus programs.

A specific section to discuss the results is presented in section 9.3

3.4. Web Credentials

When all standard user is affected, the bulk gains global proportions. The research focuses on treating user login information (usernames and passwords) by major websites that provide services such as search, home banking, e-mail and e-commerce to provide important details about how sites manage their users' passwords at the client side (Ruiz, et al., 2017). Many different bank and retail websites have been tested and found to be vulnerable to password leakage showed in Table 10.

This research (Ruiz, et al., 2017) explores the third class (OH, 2011), generating signatures for the visited websites and show how credentials are found as clear text in non-volatile memory. These signatures permit that it makes it possible to

find the usernames, bank accounts, e-mails, and passwords for the catalogued websites. (Ruiz, et al., 2017)

When the site failed to hide its login data, it was possible to extract the password. This occurred with all browsers tested (Opera, TOR, IE, Chrome, Firefox, Safari and Edge), which means that Gmail, Amazon, eBay, Santander, Hotmail, Caixa, and Citi bank websites showed the same vulnerability. (Ruiz, et al., 2017)

This research produced a signature database as seen in Table 5 that permits recovery of the entire credentials of home banking, e-commerce, social media, e-mails, and government and military web-based systems around the world.

Table 5 - Signatures

Web Site	Signature to search credentials
Hotmail	login=
Gmail	google.com/ServiceLoginAuth
Ebay	kgct=&userid=
Santander	hdnPluginOK=&txtNome=
Amazon	&mail=

Figure 10 shows the user's password as clear. The password, in this case, is “SENHACITI” this string is equivalent to “PASSWORD + CITI” in English. The method to discover the signatures consists of access to the website and a impute a known user and password. Also find this keyword in the machine using HinHex or Strings. When the keyword is founded, is possible to analyse the key to establish a signature. It permits locate unknown credentials when you have access to any machine

that the victim was used on the target website. In a real experiment, I can able to get access to my sister Santander bank account and transfer one dollar to my account for the good of science. She was received instructions to make secure transactions after this and give me the dollar as a donation.

Table 6 Setup test

T est name	Description	Sites Tested
A	Consists, on a virtual machine with Safari 5.1.7_1 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
F	Consists, on a virtual machine with Firefox 24.0_1, installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
G	Consists, on a virtual machine with Google Chrome 30.0.159969M_1 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com,

		ebay.com, santander.com.br, walmart.com.br and caixa.com.br
M	Consists, on a real machine with Internet Explorer 10 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
A C	Consists, on a virtual machine with Android 4.0.3 and web browser Robot installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
O	Consists, on a virtual machine with Opera 27.0.16.89.69 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
T	Consists, on a virtual machine with Tor Browser, installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com,

		ebay.com, santander.com.br,
		walmart.com.br and
		caixa.com.br

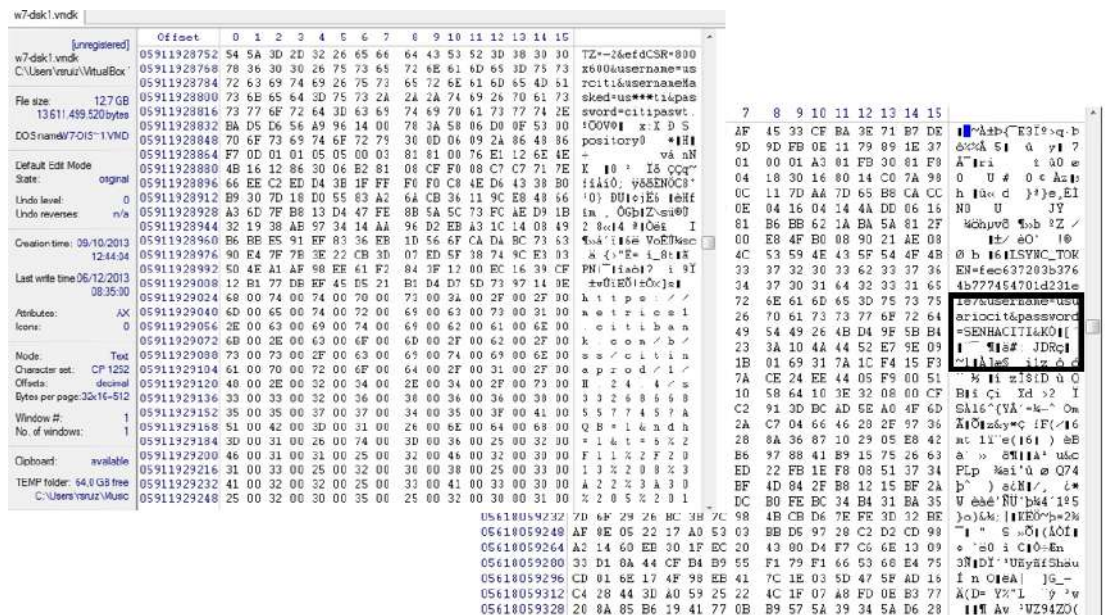


Figure 12 - Citi bank home banking

A specific section to discuss the results is presented in section 9.4

3.5. Cyber Security Education

This section provides a critical survey of cyber security education status in UK Universities and provides a method to classify how relevant is cyber security in this environment.

The data presented demonstrate that teaching Cyber Security content is flawed in the UK. Only a few interested in specializing in the field attend these classes and, in general, are already looking for specialized courses to train Cyber Security specialists.

It is important to emphasize that this study intends to demonstrate the need for all know about Cyber Security, whether as mere users, as specialists, or mainly in this study's focus as software developers.

Trying to change this reality, this study offers the community an evaluation index that can indicate the universities most committed to a curriculum rich in Cyber Security, able to return to society, less vulnerable software and mainly a culture of security and privacy instilled in the habits of their students that will be disseminated throughout British society.

3.5.1. Cyber Security Education in UK

Computer Science Courses

To understand how the universities in the UK are thinking about Cyber Security is necessary to analyse the curriculum of the offered courses. However, is a need to see the common basis courses and discard Cyber Security courses. **The intention is not to evaluate Cyber Security specialists; however, study the impact of the lack of study of the discipline base on computer science knowledge.**

After reading the discipline components of 100 UK Computer Science courses G400 or similar to extract valuable information about Cyber Security priority in the UK. (Ruiz, 2019) Table 7 shows the resume of the dataset.

Table 7 - Collected data extracted by reading course descriptions provided by each institution on their own curricula description. (Ruiz, 2019)

Totals	Amount
Courses	100
Security content	189
Optional security content	81
Mandatory security content	108
Courses without security content	13
Courses without mandatory security content	39
Security content in the year 1 of courses	32
Security content in the year 2 of courses	43
Total security content in year 3 or later of courses	114

3.5.2. IRCS (Index of Relevance in Cyber Security)

To help society to improve more quality into Cyber Security education and receive more quality in software development this research proposes an index to qualify G400 courses in the UK.

Based on G400 public curricula provided by UK Universities, this research was found word or expression linked to security was found during the reading of a discipline's menu.

Annotations have also been made by the author also made to identify at which

point in time, the safety element was addressed, as well as whether the subject discipline was mandatory or optional.

This IRCS (Index of Relevance in Cyber Security) index proposes to privilege the mandatory content and the content given at the beginning of the course. The more mandatory Cyber Security content and the more Cyber Security content in the first year of the course, the higher the index.

MC = Mandatory content;

OC = Optional content;

FYC=First year content;

SYC=Second year content;

LYC=Latest year content 3 or more.

The IRCS is calculated following the formula below:

$$IRCS = \sum MC * 1 + \sum OC * 0.2 + \sum FYC * 1 + \sum SYC * 0.3 + \sum LYC * 0.15$$

Table 8 provides a list of 100 UK Universities that offer G400 or very similar courses. Column (a) show the UK ranking, (b) World Ranking according to (Cybermetrics, 2018); (c)IRCS (Index of Relevance in Cyber Security), (d) University; (e) Total of Cyber Security content; (f) Total of Cyber Security content taught as optional; (g) Total of mandatory Cyber Security content; (h) Total of Cyber Security content in the first year; (i) Total of Cyber Security content in the second year; (j) Total of Cyber Security content in the third year; (k) Total of Cyber Security content in the fourth year; (l) Total of Cyber Security content in the fifth year; (m) Total of Cyber Security content in the sum of last 3 years.

A specific section to discuss the results is presented in section 9.5.

Table 8 IRCS - Index of Relevance in Cyber Security 2019, dataset.

Ranking		IRCS	University	Total	Optional Discipline	Mandatory Discipline	Year of Course					3+4+5year
UK	World						1	2	3	4	5	
a	b	c	d	e	f	g	h	i	j	k	l	m
97	1505	9,2	Robert Gordon University	8	0	8	0	0	8	0	0	8
114	2251	5,1	University of Winchester	4	1	3	1	3	0	0	0	0
35	361	4,6	University of Liverpool	4	0	4	0	0	4	0	0	4
83	1090	3,65	Lincoln University	3	1	2	1	1	1	0	0	1
47	617	3,45	Bangor University	3	0	3	0	0	3	0	0	3
52	669	3,45	University of Portsmouth	3	0	3	0	0	3	0	0	3
67	846	3,3	De Montfort University	2	0	2	1	1	0	0	0	0
94	1447	3,3	University of Bedfordshire	2	0	2	1	1	0	0	0	0
79	1047	3,15	University of Bradford	2	0	2	1	0	1	0	0	1
39	420	2,65	University of Kent	3	1	2	0	0	3	0	0	3
98	1512	2,6	University of Derby	2	0	2	0	2	0	0	0	0
32	342	2,45	University of Reading	2	0	2	0	1	1	0	0	1
102	1738	2,45	Edge Hill University	2	0	2	0	1	1	0	0	1
1	7	2,3	University of Oxford	2	0	2	0	0	1	1	0	2
41	521	2,05	University of Plymouth	5	5	0	0	2	3	0	0	3
69	866	2	University of Central Lancashire	1	0	1	1	0	0	0	0	0
72	899	2	Bournemouth University	1	0	1	1	0	0	0	0	0
89	1359	2	London Metropolitan University	1	0	1	1	0	0	0	0	0
109	2000	2	University of Abertay	1	0	1	1	0	0	0	0	0
110	2135	2	University of Sunderland	1	0	1	1	0	0	0	0	0
12	138	1,9	Bristol University	3	3	0	1	0	2	0	0	2
95	1471	1,9	Staffordshire University	3	3	0	1	0	0	2	0	2
17	177	1,65	University of Birmingham	2	1	1	0	1	1	0	0	1
62	795	1,65	University of Salford	2	1	1	0	1	1	0	0	1
9	97	1,5	University of Leeds	2	1	1	0	0	2	0	0	2
56	713	1,5	University of Ulster	2	1	1	0	0	1	0	1	2
57	718	1,5	University of Hertfordshire	2	1	1	0	0	2	0	0	2
50	641	1,4	University of Stirling	4	4	0	0	0	0	4	0	4
2	10	1,3	University of Cambridge	1	0	1	0	1	0	0	0	0
18	185	1,3	University of Exeter	1	0	1	0	1	0	0	0	0

64	825	1,3	Oxford Brookes University	1	0	1	0	1	0	0	0	0
73	914	1,3	University of Huddersfield	1	0	1	0	1	0	0	0	0
88	1295	1,3	University of South Wales (Glamorgan & Wales Newport)	1	0	1	0	1	0	0	0	0
93	1443	1,3	Teesside University	1	0	1	0	1	0	0	0	0
99	1583	1,3	Birmingham City University (University of Central England)	1	0	1	0	1	0	0	0	0
54	700	1,2	Keele University	1	1	0	1	0	0	0	0	0
7	78	1,15	King's College London	1	0	1	0	0	1	0	0	1
26	304	1,15	Lancaster University	1	0	1	0	0	1	0	0	1
58	720	1,15	Aston University	1	0	1	0	0	0	1	0	1
63	814	1,15	Goldsmiths University of London	1	0	1	0	0	1	0	0	1
90	1381	1,15	University of East London	1	0	1	0	0	1	0	0	1
92	1408	1,15	London South Bank University	1	0	1	0	0	0	1	0	1
108	1961	1,15	Cardiff Metropolitan University (University of Wales Institute Cardiff)	1	0	1	0	0	0	1	0	1
37	391	1,05	Loughborough University	3	3	0	0	0	3	0	0	3
40	443	1,05	Brunel University	3	3	0	0	0	3	0	0	3
44	536	1,05	City University London	3	3	0	0	0	3	0	0	3
5	56	0,7	Imperial College London	2	2	0	0	0	0	2	0	2
13	145	0,7	University of Southampton	2	2	0	0	0	2	0	0	2
15	148	0,7	Newcastle University Newcastle upon Tyne	2	2	0	0	0	2	0	0	2
16	167	0,7	University of Sheffield	2	2	0	0	0	1	1	0	2
22	208	0,7	Cardiff University	2	2	0	0	0	2	0	0	2
76	945	0,5	Kingston University London	1	1	0	0	1	0	0	0	0
6	65	0,35	University of Manchester	1	1	0	0	0	1	0	0	1
10	120	0,35	University of Warwick	1	1	0	0	0	1	0	0	1
11	136	0,35	University of Nottingham	1	1	0	0	0	1	0	0	1
14	146	0,35	Queen Mary University of London	1	1	0	0	0	1	0	0	1
23	246	0,35	University of Leicester	1	1	0	0	0	1	0	0	1
24	269	0,35	University of Saint Andrews	1	1	0	0	0	1	0	0	1
29	319	0,35	University of Surrey	1	1	0	0	0	1	0	0	1
30	322	0,35	Queen's University Belfast	1	1	0	0	0	1	0	0	1
55	705	0,35	University of the West of England	1	1	0	0	0	1	0	0	1
60	749	0,35	Manchester Metropolitan University	1	1	0	0	0	1	0	0	1
103	1787	0,35	University of Chester	1	1	0	0	0	1	0	0	1
3	19	0	University College London	0	0	0	0	0	0	0	0	0

4	41	0	University of Edinburgh	0	0	0	0	0	0	0	0	0
8	92	0	University of Glasgow	0	0	0	0	0	0	0	0	0
20	201	0	Durham University	0	0	0	0	0	0	0	0	0
21	206	0	University of York	0	0	0	0	0	0	0	0	0
25	283	0	University of Aberdeen	0	0	0	0	0	0	0	0	0
27	309	0	University of East Anglia	0	0	0	0	0	0	0	0	0
28	310	0	University of Sussex	0	0	0	0	0	0	0	0	0
31	323	0	University of Bath	0	0	0	0	0	0	0	0	0
36	386	0	University of Strathclyde	0	0	0	0	0	0	0	0	0
42	526	0	Heriot-Watt University	0	0	0	0	0	0	0	0	0
43	528	0	University of Essex	0	0	0	0	0	0	0	0	0
45	557	0	Swansea University	0	0	0	0	0	0	0	0	0
46	579	0	Royal Holloway University of London	0	0	0	0	0	0	0	0	0
48	634	0	Aberystwyth University / Prifysgol Aberystwyth	0	0	0	0	0	0	0	0	0
49	637	0	Cranfield University	0	0	0	0	0	0	0	0	0
51	644	0	Birkbeck University of London	0	0	0	0	0	0	0	0	0
53	681	0	University of Hull	0	0	0	0	0	0	0	0	0
59	731	0	Northumbria University	0	0	0	0	0	0	0	0	0
61	785	0	University of Brighton	0	0	0	0	0	0	0	0	0
65	829	0	Sheffield Hallam University	0	0	0	0	0	0	0	0	0
66	841	0	Liverpool John Moores University	0	0	0	0	0	0	0	0	0
68	855	0	Nottingham Trent University	0	0	0	0	0	0	0	0	0
71	895	0	University of Greenwich	0	0	0	0	0	0	0	0	0
74	934	0	Middlesex University	0	0	0	0	0	0	0	0	0
77	967	0	Coventry University	0	0	0	0	0	0	0	0	0
78	973	0	University of Westminster	0	0	0	0	0	0	0	0	0
80	1068	0	University of Wolverhampton	0	0	0	0	0	0	0	0	0
84	1137	0	Glasgow Caledonian University	0	0	0	0	0	0	0	0	0
85	1238	0	Anglia Ruskin University	0	0	0	0	0	0	0	0	0
86	1248	0	Napier University Edinburgh	0	0	0	0	0	0	0	0	0
91	1386	0	Leeds Beckett University (Leeds Metropolitan University)	0	0	0	0	0	0	0	0	0
104	1810	0	Canterbury Christ Church University	0	0	0	0	0	0	0	0	0
105	1849	0	University of Bolton	0	0	0	0	0	0	0	0	0
106	1916	0	University of Gloucestershire	0	0	0	0	0	0	0	0	0
107	1948	0	University of Northampton	0	0	0	0	0	0	0	0	0
111	2172	0	University of Worcester	0	0	0	0	0	0	0	0	0
Totals				118	55	63	13	22	69	13	1	83

4. Privacy

4.1. Introduction

Considering that the rich and most influencer corporations inside the software market are concerned with the problems (all of them sell anti malware software, and is present in EU and need to care about EU privacy regulations) that this research exposes to propose the best solution for society. Those organizations are looking for first-class experts. Besides, even though these experts in trendy come from satisfactory universities. It makes the best feel to question standards and curricula in analysing the interdependence among entities of Cyber Security. To exemplify, this chapter will discuss the “*incognito* mode” or “*InPrivate* mode” used in web browsers.

Before, everything is an ancient and monetary difficulty that has been with us since the first software until today. The truth is that the basis of present-day software was created in an insecure manner. The concept of safety turned into to require a whole

lot later. This original vulnerability in the DNA of each running system and software program based on that Operational System has been maintained considering since start and without an actual evolution especially because of the economic impacts of starting over.

An inverted pyramid Figure 1 intends to present the instability of all these small Environments and the educational system's responsibility for a better future in the cybernetic area. Cyber Security in The First Line of the First Code is the best choice to have better Cyber Security in the next decades.

4.2. Author's Contributions to Privacy

For the study, the collected vendors' promises on private browsing and exploring aspects of the user's privacy.

This paper summarizes the following:

Turning Public the private navigation at The Seventh International Conference On Forensic Computer Science - ICOFCS 2012, Brasilia, Brazil (Ruiz, et al., 2012);

As the focus is to assess the functionality of private browsing in isolation, it is considered that the user does not adopt security techniques that could potentially influence access to the data generated during navigation. In the four types of tests performed, it is possible to verify that the tested version of Internet Explorer has serious flaws in its private browsing functionality by making available in the system a series of information that would make it possible not only to identify visited pages but

also to reconstruct them. Thus, it can be concluded that for the methodology adopted, the private browsing functionality implemented in Firefox is more adequate than that found in Internet Explorer. This work proposed and perform a method to recover images and data after *InPrivate* navigation.

- Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

Opening the “ Private Browsing “ Data – Acquiring Evidence of Browsing Activities at Proceedings of the International Conference on Information Security and Cyber Forensics, 2014 Kuala Terengganu, Malaysia (Ruiz, et al., 2014);

After the repercussion of the first work of private browsing, this work present adjusts the method and improve the tests in a real machine to resolve any doubts about possible differences between a virtual machine and a real machine. Criticisms of previous work maintain that the behaviour of browsers on virtual machines would be questionable.

- Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

Overconfidence: Personal Behaviours Regarding Privacy that Allows the Leakage of Informations in Private Browsing Mode at International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2015 (Ruiz, et al., 2015);

Many lectures later, some citations and new products in the market were the motivation for this work. New improvements are imputed in this new version of the method to test private browsing, make operations to interact with the site, and finish the browser's execution correctly and abnormal, including simulating a power outage

- generating the virtual machine image for analysis. The famous TorBrowser and Opera browser, IE10 and Android Chrome were added, tested and failed like others.

- Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

Privacy in The First Line of the First Code, Science Magazine, 2020 (Ruiz, et al., 2020);

This paper explores the relations of privacy issues whit Computer Science courses in the UK. For this purpose, the text use citations of many previously published works linked in the same scope.

- Individual contribution: Principal researcher and writer advised by Prof. Kazemian and Dr. Shukla.
- The results obtained for the browser tests are grouped in Table 9. The result can be Yes when data is found, no when data was not found, and n/a when the test cannot be applied:

The method presented in section 3.1 show that browsers tested are unable to provide privacy in various situations demonstrated in Table 9.

- *Table 9 - In private mode test results.*

Recovery	F Test	K Test	P Test	S Test	Browser
Page address	Yes	Yes	Yes	Yes	Safari
	Yes	Yes	Yes	Yes	Firefox
	Yes	Yes	Yes	Yes	Chrome
	n/a	n/a	n/a	Yes	Tor Browse
	n/a	n/a	n/a	Yes	Chrome/A ndroid 4.0.3
	Yes	Yes	No	Yes	IE10
Picture	No	Yes	Yes	Yes	Safari
	No	Yes	Yes	Yes	Firefox
	No	Yes	Yes	Yes	Chrome
	n/a	n/a	n/a	Yes	Tor Browse
	n/a	n/a	n/a	Yes	Chrome/A ndroid 4.0.3
	No	No	Yes	No	IE10

4.3. Summary

The concept of privacy is very new in humankind's history, and it is becoming more and more relevant the more significant the society and group where the person lives. A different culture is having other concepts of what needs to be private.

This chapter intended to show how society can lose privacy and sensitive data on the internet with false vendor promises and wrong orientations. Also, this chapter explores test software issues and the relation between teaching and harmful software developed.

This chapter was contributed with three versions of a method to restore *incognito/InPrivate* mode navigation, able to expose all navigation made over *incognito* mode. The method works over browsers like IE, Edge, Firefox, Safari, Chrome, Opera and TOR over Windows systems. It is relevant to use in crime labs that investigate suspicious activities in the suspect machine. In the next chapter a special element of cryptography is explored, the key management.

5. Encryption

5.1. Introduction

This work presents methods to bypass famous cryptographic programs to gain access to private data. Possible scenarios will be presented, and the origins of the failures are discussed.

The famous and open software Truecrypt is still widely used today, even a few years since its official closure. With its interruption, a huge range of other brands continued using their original codes. Among these descendants, Veracrypt stands out. The differences of these descendants to its predecessor are only aesthetic and the file system is the same, which means that every loophole found in one of them can be applied without restrictions in the others.

There is a special motivation for every Brazilian who works with Digital Forensics. A very famous case of a banker who managed to get away with all the accusations because officially it was never possible to open the containers containing

the alleged corruption data. These data were protected by Truecrypt and PGP and not even with the help of the American FBI agency it was possible to unravel the case (Ruiz & Winter, 2017). Some people are examples of good practices in the use of Information Technology and Communication resources, like as Daniel Dantas (Satyagraha) and Marcelo Odebrecht (Ruiz & Winter, 2017) as great personalities in the management of information security. Their success begins in the consciousness about having sensitive data and the need to protect them. Next, these persons learned to control the mouth. A secret that many people know, it is no secret. Mark Twain said, *"We ought to never do wrong when people are looking"*

This chapter is composed of three specific sections to discuss Truecrypt, Bitlocker and BitDefender and the last to discuss PGP Symantec Encryption Desktop. In each one, a method is proposed to gain access to the encrypted container.

5.2. Author's Contributions to Encryption

Another point investigated was the use of cryptographic software as detailed in the papers:

Security Issue on Cloned TrueCrypt Containers and Backup Headers, The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), 2014, Kuala Lumpur, Malaysia (Ruiz, et al., 2014);

Truecrypt is open programming that guarantees security utilizing cryptographic calculations and perceived worldwide and with much acknowledgement among IT experts, this free programming is utilized both by people and by different administrative and undertakings worried about the privacy of their information. The

work proposes a strategy to sidestep the key administration arrangement of Truecrypt, propose a potential situation, and show by tests the accomplishment of the technique. The outcomes got with the proposed procedure show that Truecrypt's sharing holders aren't training that can be approved as protected since the substance inside can be gotten by any individual who approaches the first header.

- Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

Corrosive Secrecy And Confidence: The Paradox Among Bypassing Cryptographic Software, Cyber Security Review Magazine, 2016 (Ruiz & Winter, 2016);

After the good repercussion of the paper about Truecrypt (Rodrigo de S. Ruiz et al., 2014), this work finds security flaws in other renowned encryption systems in the international market – Bitlocker (Microsoft) and Bit Defender Total Encryption 2015 (Bitdefender). Likewise, the R2K test method's goal is to identify possible weaknesses in the cryptographic systems that undermine the availability, integrity, confidentiality, and authenticity of the information. The method used in the tests can be applied generally and consists of four stages: research, test, test result and dissemination.

- Individual contribution: Production of 30% of the text, creation of forensic method and conduction of laboratory tests.

Lazarus: Data Leakage with PGP and Resurrection of the Revoked User, Journal of Cyber Security and Mobility, 2016 (Ruiz & Winter, 2016).

It is the last text of the series of bypassing of the cryptographic system to

complete the verifications of all the most relevant cryptographic software in the market. In the name of this work, “Lazarus: Data Leakage with PGP and Resurrection of the Revoked User”. The title is a biblical comparison of Lazarus history, concerning his arrival from death after a miracle. In the same way, it can resuscitate a user revoked by the system owner. In this intricate sociotechnical environment of Cyber Security, this paper describes a method and discloses a flaw in Symantec Encryption Desktop (SED). In this situation, as a sample, the National Aeronautics and Space Administration (NASA) usages the Symantec Pretty Good Privacy (PGP) Encryption Desktop (SED). After contact NASA, the vendor has contacted the author to help them to reproduce the bypassing and open the case SSG15-044.

- Individual contribution: Production of 50% of the text, creation of forensic method and conduction of laboratory tests.

To Forbes (Greenberg, 2010), Symantec paid \$300Million for PGP technology. Symantec Company was notified about this research by protocol SSG15-044. National Aeronautics and Space Administration (NASA, 2012) uses the encoding system of Symantec PGP Figure 13 and also be notified, (Corbin, 2016), mentions that compliance is not the only way to ensure the security of systems.



Figure 13 - NASA screenshot with instructions about use PGP file encryption.

Symantec Company becomes a world leader in the Cyber Security market, and its systems are used in thousands of government agencies, businesses, and the military

(Ellacott, 2014).

Cyber Security is more complicated than the simple use of cryptographic software, and people are living with the wrong logic of security using a vulnerable system with an unsafe attitude. The human factor is the more important aspect in the use of this kind of software. This work is limited by the versions of software tested.

In the next chapter the web credential management is explored.

5.3. Summary

The purpose of this chapter was to explore failures in credential management used in the most famous and prestigious encryption software available in the global market. For this, it was provided three methods to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods. It is relevant to use in crime labs that investigate suspicious activities encrypted in the suspect hard drive.

Beyond software problems, it is visible problems in the environment, process, and people training. Universities (University of Michigan, 2018) (Wake Forest University, 2014) (Wake Forest University School of Business, 2018) define unsafe process sharing passwords of crypto containers and induce the researchers and students to create unsafe memories that will be used in other kinds of software and processes in their lives.

Billionaires' industry and government secrets are unsafe too when the process is transported from the university experiences for companies where university students are working and will be future collaborators. There is a direct link between the way students are trained and the safety of systems and that directly affects society's whole.

For a biochemistry student, the effect of a loss of sensitive data can affect himself or his company (Smith, 2003). Nevertheless, the effects of a computer science student's low and inadequate training in the safe use and safe programming techniques can have damaging effects in all areas of knowledge. These professionals create the tools used by all other areas of society, significantly raising their responsibility. It is possible to trace a parallel with the pandemic of COVID-19 closing schools published by OECD in September 2020. The conclusion of the report is that the student is not exposed to the appropriate content. The losses are great for the student and also for society that loses with their lack of training. (Hanushek & Woessmann, 2020).

This research does not discuss excellent mathematical algorithms. It focuses on identifying and exploring programming flaws in the management of the credentials necessary to use these mathematical algorithms as shown in chapters 3.2.1, 3.2.2 and 3.2.3. In summary, this work does not break into the safe; it simply uses techniques to locate where the user keeps the keys. Published articles (Winter & Ruiz, 2016) (Ruiz, et al., 2014) (Rodrigo Ruiz, 2017) demonstrate that this has been done with considerable success.

This chapter was provided three methods to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods. It is relevant to use in crime labs that investigate suspicious activities encrypted in the suspect hard drive.

6. Web Credentials

6.1. Introduction

The investigation sequence occurs when the internet's standard user uses any kind of credentials on the web. Each day, people put their credentials in social media, at e-commerce, to buy flowers, food or vehicles, and company shares in New York Stock Exchange and home banking to pay bills and do other bank transactions.

The continuing assessment of operating systems, browsers and cryptographic programs has already generated many disclosures about security breaches and failures. The present section emphasises the treatment of user login information (user-names and passwords) by major websites that provide services such as search, home banking, e-mail and e-commerce. The data gathered for the present research provide important details about how these sites manage their users' passwords on the client side. Many different bank and retail websites have been tested and found to be vulnerable

to password leakage. This work starts with a discussion on threats and vulnerabilities, and discusses other research and methodological treatments in the context of this topic. Are described the methods and tests used in this study. The results obtained by the tests are then presented and discussed. Finally, conclusions are drawn and recommendations for further studies are proposed.

Table 10, the present research focuses on the treatment of credentials by relevant websites such as search, home banking, e-mail, and e-commerce. Table 10 was based on the UK Standard Industrial Classification (UK SIC) Codes (Office for National Statistics UK, 2016)

Table 10 - Tested sites.

<i>Domain</i>	<i>Economic Activity</i>
gmail.com	Information and communication
hotmail.com	Information and communication
yahoo.com	Information and communication
amazon.com	Retail trade
paypal.com	Financial and insurance activities
ebay.com	Retail trade
santander.com.br	Financial and insurance activities
walmart.com.br	Retail trade
bradesco.com.br	Financial and insurance activities
citibank.com.br	Financial and insurance activities
citibank.com	Financial and insurance activities
jpmorgan.chase.com	Financial and insurance activities
particulares.gruposantander.es	Financial and insurance activities

The results showing an interesting vision about how those sites manage their user's credentials on the client side.

6.2. Author's Contributions to Web Credentials

This chapter is based on one article:

The Leakage of Passwords From Home Banking Sites: A Threat to Global Cyber Security? At Journal of Payments Strategy & Systems, 2017. (Ruiz, et al., 2017)

E-banking frameworks depend on programs and other money-related applications to offer safe support. As this paper appears, nonetheless, numerous e-banking frameworks neglect to give the imperative degree of classification. This paper centres around vulnerabilities identified with the spillage of login data from the customer side. It shows that it was conceivable to obtain login-related information from a few sites by utilizing legal strategies and instruments. It shows that significant validation information utilized in route exercises stay on a circle, representing a reasonable danger to privacy. The technique introduced in this work can discover as clear content, all client accreditations as clear content, including the secret word. Before the distribution of this paper, numerous Brazilian banks were fixed the issue after contacted by the author.

- Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

How easy is it to gain access to user credentials? All tests setups are summarized in Table 6. To find answers this study were performed seven different tests in some browsers: Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1, Safari 5.1.7_1, Opera 27.0.16.89.69, Robot 4.0.3 and Tor Browser 4.0.4.

In Figure 14 as seeing Gmail⁴ full opened credentials. Suppose the company that is a model for all in internet stuff have this kind of security problem. How is it possible to expect security from small and medium-sized companies and even from governments?

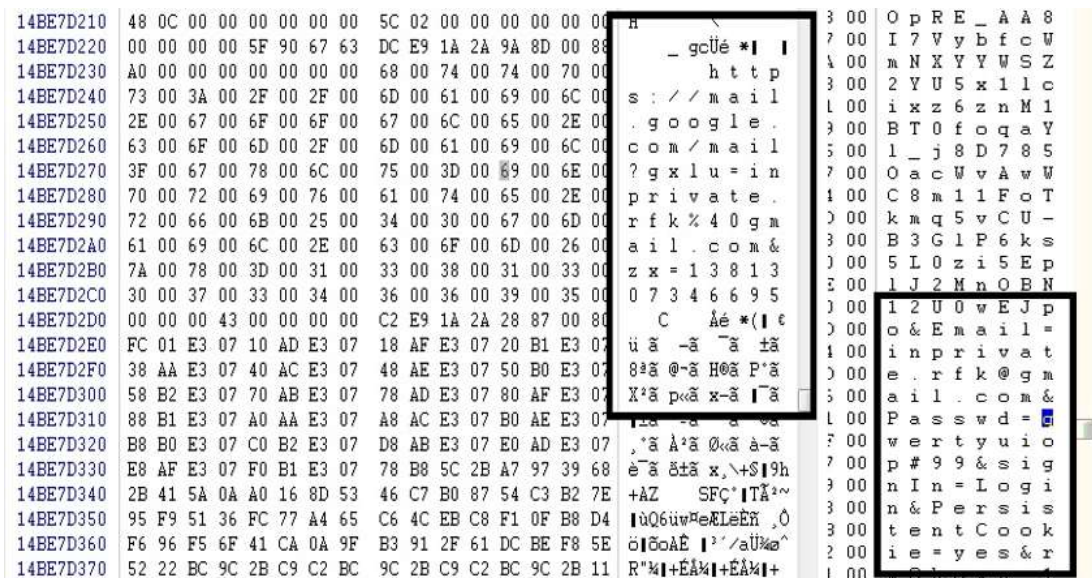


Figure 14 - Gmail full opened credentials.

About private browsing (Ruiz, et al., 2014) apply signatures and string matching to extract data related to visited websites after in private navigation.

What happens if a notebook is stolen?

Also, consider this basic HTML form:

```
HTML code
<form method="POST" action="">
  <br>User : <input type="text" name="user" size="20">
  <br>Password: <input type="password" name="password" size="20">
  <br><input type="submit">
</form>
```

⁴ Gmail.

6.3. Summary

In this chapter, the side effect most directly applied to the fears of society and ordinary citizens was presented. It was explained how an attacker can obtain credentials and have access to a user bank account, make improper purchases in a third person name, have access to user emails, and recover many other accounts for access to various services. Web Credentials chapter was explored how to get clear text credentials after the analyst having access to the computer target. The proposed method can get credentials used in intranets or e-commerce, home banking and email accounts. It can be used in criminal investigations or to improve more strong security in these websites.

In more specific and targeted cases, access to specific systems of government, companies, and even the military and law enforcement can be done, generating irreparable damage for the whole of society.

A worrying fact was the attitude of the contracted companies, which mostly preferred to ignore the fact. This may be due to a standard postponement procedure for any image damage. If a bank were to suffer a similar attack, it would resort to the insurance system, reimburse the client individually by covering up the case and avoiding the expenditure of thousands of pounds to correct the systems, train its staff and run the risk of mere vulnerability information leaking to the market. Denying costs less than to publicly admit insecurity in their structures. In Brazil and many other places the appearance is more important than real facts. If a bank's image is tarnished by the admission of a burglary by hacking into its systems, the drop in the value of its

stock on the stock exchange is several times greater than the robbery itself. In the next chapter the author explores security systems and how they can be used against the users.

7. Security Systems

7.1. Introduction

When the human body is an inspiration, this chapter remembered autoimmune diseases to use this concept for the first related time into Cyber Security. “*Autoimmune diseases result from a loss of self-tolerance and the consequent immune destruction of host tissues*” (Zhao, et al., 1998) pp 1344. Exists some suspects that viral infection can induce or aggravate autoimmune diseases (Zhao, et al., 1998).

To confront this threat, the most famous group of security software is the antivirus that was created based on the observation of the human immune system the author has created the Apoc@lypse Technique (Ruiz, et al., 2015) (Winter & Ruiz, 2017) (Ruiz, et al., 2016) (Ruiz & Winter, 2015). The technique uses the human body, natural virus, and bacteria analogy. It is based on the injection of any DNA fragment of a computer virus in benign files, without necessarily interfering with these files' functionality. Within the Apoc@lypse Technique can use three forms of viral DNA

injection in a file: Injection with total replacement of the file contents, injection at the beginning of the file, and injection at the end of the file.

This chapter explores three-decade-old engines used to protect systems around the world. The signature method will be asked and scenarios will be proposed. This work will use the EICAR test file to induce a cyber autoimmune disease. Present from more than 30 years, generation by generation of all family antimalware software, the Cyber Autoimmune Disease may cause critical damage to critical infra-structure around the World. Viruses are a major threat to Cyber Security and the health of people. Viruses that attack computers and humans have stimulated great research and they are difficult problems to solve. The digital world has an evolution rule similar to humans, like Darwinian evolution. Computer viruses as well as human viruses have evolved over the years. Computer Viruses are human creations and they are the product of their creativity and ingenuity. Inspired by the concepts of viral infection and prophage this research found a way to start an autoimmune disease in an antivirus system. Thereby, after started the cyber autoimmune disease, the antivirus system is responsible for destroying the computer's operating system. The proof of concept was called Apoc@lypse Technique and it will be presented below.

“Viruses are the most abundant parasites on Earth” (National Science Foundation 2011). Well-known viruses, such as the flu virus, attack human hosts, while viruses, such as Sasser, Conficker, and Stuxnet infect a computer. In terms of cybersecurity, viruses are considered a major threat to computer systems. Fred Cohen, who is best known as the inventor of computer virus and defence techniques, pointed out that viruses were one of the biggest problems the security of computers in 1987. Cohen defined "computer virus" and demonstrated that no algorithm could detect perfectly all the possible viruses. Cybersecurity has grown in importance but is

possible to observe that defence systems are not effective to prevent attacks. The human body suffers attacks from viruses and bacteria, hence ever depending on more efficient drugs to combat them.

There is a remarkable similarity between the virtual world and the real world, perhaps because the problems related to the vast majority of computing solutions have been inspired by the observation of nature itself. What has called attention is the possibility of evolution of cyber viruses as it occurs in nature. Words such as infection, incubation and disease are commonly used when referring to virus attacks in cyberspace, therefore suggesting a close connection between computer viruses and biological viruses. This analogy is a logical condition that was explained by Eric Filiol, in one of his publications in 2005.

In the book "Computer Viruses, Artificial Life and Evolution" (M. A. Ludwig 1993), its author posed some comments on the possibility that computers can simulate life or artificial life. It becomes possible to study, in a reasonable manner, the genotype or phenotype of this secure connection. Furthermore, in "The Giant Black Book of Computer Viruses" (M. Ludwig 1995), the author states that the best approach to attack a computer system is to create an entity capable to emulate the essence of a gene behaviour, aiming at launching a Darwinian evolution process. When an antivirus system (AV) eradicates virus samples, the whole virus population learn how to protect itself from the AV. This phenomenon can be recognized as a simple 'Darwinian evolution'-like process. Might it establish a relationship between the protection of any computer system and the human body immune (defence) system?

It is clear that malware problems are difficult to solve and have caused great financial losses for companies, governments, the military and common citizens over the last 40 years. However, antivirus companies have been developing several

technologies to combat several viruses. It is an endless struggle to fight an enemy that continues growing and evolving – much like a virus does. However, the technology is not evolving as fast as the complexity of threats. According to Richard Ford (Ford 2004) “While the antivirus industry has been steadily improving over the years, it may come as a surprise for some to realize that the fundamental technology used for detecting and removing viruses has changed very little over time”.

In the present research, it is possible to demonstrate that the statements of (Ford 2004) are still valid for the antivirus systems. This research found that viral infection in a cyber ‘body’ is the perfect trigger to start a cyber autoimmune disease. The article presents the Apoc@lypse technique (Ruiz, et al. 2015) and the harmful effects it onto computer systems. It also establishes a close relationship between human autoimmune diseases and cyber autoimmune diseases. The Apoc@lypse technique has been inspired by reading reports of several scientists, who have studied medical phenomena, such as viral infection, autoimmune diseases and bacteriophage. Apoc@lypse technique is equivalent to ‘program’ a bacteria to make a given maleficent behaviour, using a technique inspired by the bacteriophage, to carry a virus fragment up to cells of a human body. After this, the antivirus system starts to interpret mistakenly the given piece of harmless code as a threaten/attack – that otherwise would not represent any problem should this misunderstanding do not happen – and initiate the destruction of what erroneously is interpreted by the AV as infected files.

Nowadays, viruses are considered a subclass of malware. According to DHS, Malware refers to a broad class of attack software or hardware that is loaded on machines, typically without the knowledge of the legitimate owner, that compromises the machine to the benefit of an adversary (Department Homeland Security 2009), pp. 38. McAfee catalogued over 100,000 new malware samples every day, late in 2013

(McAfee Company 2013). In this article, ‘antivirus’ and ‘antimalware’ are used interchangeably, as antivirus is a well-known word, as virus and malware.

Over the past ten years, malware has been used as a cyber weapon, being its study part of the research efforts related to military operations, defence from cybercrimes and cyberespionage operations. For instance, in 2010, the Stuxnet malware was used for the first large-scale attack on Supervisory Control and Data Acquisition (SCADA) in Natanz Nuclear Plant, in Iran. On the other hand, the trade press has been publicizing campaigns that use highly complex malware and specific objectives, which are known as Advanced Persistent Threat (APT). In August 2012, a virus attack erased data kept in three-quarters of the corporate computers of the oil company Saudi Aramco (Lasiello 2015).

Antivirus systems have suffered severe criticism due to their low efficiency. Some articles in the trade press have decreed its death. What the author has described in this article is a ‘disease’ that all antivirus systems have in common – and, exactly for this common vulnerability – is exploited by the Apoc@lypse technique. The concepts that emerge in this work are autoimmune diseases and cyber autoimmune diseases. Autoimmune diseases result from a loss of self-tolerance and the consequent immune destruction of host tissues (Zhao, et al. 1998) pp 1344. The effectiveness of this destructive process, connects us, by analogy, to the question of autoimmune diseases is associated with a viral infection in cyberspace. There are indications that some viral infections can induce or exacerbate autoimmune diseases (Zhao, et al. 1998).

Researchers at the California Institute of Technology (Tadmor, et al. 2011) have been successful in statistically reduce the effects of viral infections when the virus causing the disease is specifically associated with the host – by, injecting its DNA into

the host and embedding it into the host as a prophage (a viral genome inserted and integrated into the DNA of bacteria).

Recently, scientists at Michigan State University (Parry 2012) used a virus called "Lambda", which presents extremely quick mutations (changes) and can infect a bacterium via a new 'door'. Typically, the Lambda virus is capable of infecting E. coli cells. Bacteriophage, also called phage or bacterial virus, are names given to any kind of viruses that infects bacteria (The Editors of Encyclopædia Britannica 2015), by inducing the bacteria to replicate thousands of viruses after the injection of the phage genome into the cytoplasm of the host cell

The concepts in research (Zhao, et al. 1998), (Tadmor, et al. 2011), and (Parry 2012) inspired other researchers to perform tests to explore different antivirus systems.; including us. Initially, this research applied the concept of viral infections as a means of triggering autoimmune disease. Secondly, the concept of prophage has been applied to resemble the DNA obfuscation technique used by viruses for the infection process, but in this case, injecting the computer virus' DNA into the operating system files of a computer. By doing so, this work succeeded in mapping what a computer virus gets into and from a digital bacterium.

Inside computer systems are files, commands and several kinds of programs that are known as 'benign', being understood by the installed antivirus system as such. The prophage or obfuscation ensures protection to the virus and allows it to deceive the defences of the antivirus system. Many bacteria live in the human body symbiotically, being beneficial to the human body, such as the Lactobacilli. Thus, such kinds of bacteria do not sensitize the human immune system.

More accurately, the Apoc@lypse Technique exploits a vulnerability in the

concept of what is treated by the engines of the antivirus systems as being threatening. False-positive detection (‘misdetection’) is a fundamental concept of all antivirus systems, from the earliest to the present ones. In an antivirus system, exists two main different approaches: misuse detection and anomaly detection. Misuse detection is based on signatures or patterns of attacks on the computational system. Some actions directed to the objects of the system are considered threatening, as an attempt to delete a file, or to format the hard disk or to modify privileged access grant files. Well known and defined actions against the weaker points of the given system use to form the signature of the attacks. The detection of attacks happens by observing such actions occurring onto specific objects. Conversely, anomaly detection is based on the definition of the expected behaviour of a host computer or its network. Therefore, a pattern of the normal behaviour is captured, for instance, by using statistical methods together with association rules. So, by monitoring abnormal behaviour of the system compared to the expected one, i.e., with the ‘pattern’, it’s possible to identify an attack.

7.2. Author’s Contributions to Security Systems

This chapter is based on five publications:

Apoc@lypse: The End of Antivirus, book published in 2015 and indexed by ACM (Ruiz, et al., 2015);

This ACM (ACM, 2020) indexed book presents a method capable of inducing a cyber-autoimmune disease that makes the antivirus system destroy the operational

system look like human autoimmune diseases. It was news on the websites of the Brazilian Ministry of Science and Technology as well as on the portal of the Federal Government of Brazil; it also received notes from several specialized nationals such as Computer World magazine that also commented on the book in its subsidiary in Portugal. Currently ranks number 40 in the Computer Security and Cryptography category from Amazon, and the months after its launch, it came to occupy position 44 on Amazon American, tenth place on Amazon Germany, and first place on Amazon Brazil.

- Individual contribution: Creation of method of cyber-autoimmune disease, coordination of workgroup, and write 50% of the text.

Apoc@lypse: when the antimalware is sick at Cyber Defence Magazine, 2015 (Ruiz & Winter, 2015);

Terms similar to infection, incubation, and disease in the context of information security suggest a similarity between computers and biological viruses, a logical parallel. In this way, this research established a metaphor between the human body and cyber systems, particularly system protection. Autoimmune disease happens when the human immune system has a fault, and it attacks cells and tissues of the organism itself in the same way as a virus or a bacterium tries to infect a human body. Vendors do not solve these issues yet.

- Individual contribution: Creation of method of cyber autoimmune disease and 30% of the text.

Apoc@lypse: The End of Antivirus. When The Antivirus is The Threat at

Cyber Security Review Magazine, 2016 (Winter & Ruiz, 2016);

The military field was the motivation for this work. The utilization of a cyber weapon is one way to conduct a cyber-attack. Any person can learn about and create operative cyber weapons. To do it, it is needed a computer, Internet connection, time and persistence to study software, hardware, and network vulnerabilities. This work proposes a scenario and method to create a cyber weapon to be used in Cyber Security with effects in the physical world.

- Individual contribution: Creation of method of cyber autoimmune disease and 40% of the text.

Cyber Security, Cyber Weapons And Cyber-Attacks: Responsibility and Different Reflections at Critical Infrastructure Protection Review Magazine, 2017 (Winter & Ruiz, 2017);

The motivation for this article was a request from ResearchGate(see appendix O) to provide an analysis of recent attacks in Ukrainian power plants. It concludes that all governments are contributing to insecure Cyber Security. In this game are no victims. All countries are responsible for global cyber-attacks. All countries will continue to improve their cyber weapons. The DOD should continue to prioritize its cyber investments and develop the capabilities required to defend the US, and the other countries may invest in this kind of active protection.

Individual contribution: Write 50% of the text and revise.

Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life at International Journal of Cyber-Security and Digital Forensics, 2107 (Winter & Ruiz, 2017).

This academic paper presents the full disclosure of the method to induce a

previously partial disclosure of a cyber-autoimmune disease in previous works. This work demonstrates that antivirus software is being implemented using inefficient methods and techniques to combat complex threats. This paper shows how inoffensive fragments of malware files can induce the abnormal reaction of antivirus systems destroying the operations system.

- Individual contribution: Creation of method of cyber autoimmune disease and 30% of the text.

This research separated the common aspects generally visualized by the industry, the market, and other investigators. New technologies and the most sophisticated techniques are employed to detect malware. Those things, however, are external to the antivirus nucleus. This research went back to the basic beginnings, to the DNA of the antivirus. Questioning the paradigms now consolidated in the software through four decades, this work revised the history of this software development, and started to study the common core carefully.

Bio inspiration makes us verify that the fault is in the DNA of the modern antivirus software ancestors. The basic form with which the antivirus software was created since the first one; it has transmitted its genes for generations to now. It is the equivalent of a defective chromosome passed from father to son generation after generation. Thus, the only way of preventing the disease in a new generation does not to have more descendants. (Ruiz, et al., 2015)

To demonstrate the efficiency of the method, (Ruiz, et al., 2015) was created the prototype using no more than operational system native tools, like a simple text editor, batch files and macro substitution. The prototype can execute all tasks to inoculate the DNA (inoffensive fragment of the virus) into the files and hidden from

antimalware. After the inoculation, the antivirus panics and begins to delete all files with the mark. At the same time, the antivirus destroys the system and sends a message to the user saying that everything is fine and the antivirus is protecting the user, as seeing in Figure 15. After some minutes, the system does not exist anymore, as seen in Figure 10 and Figure 11.

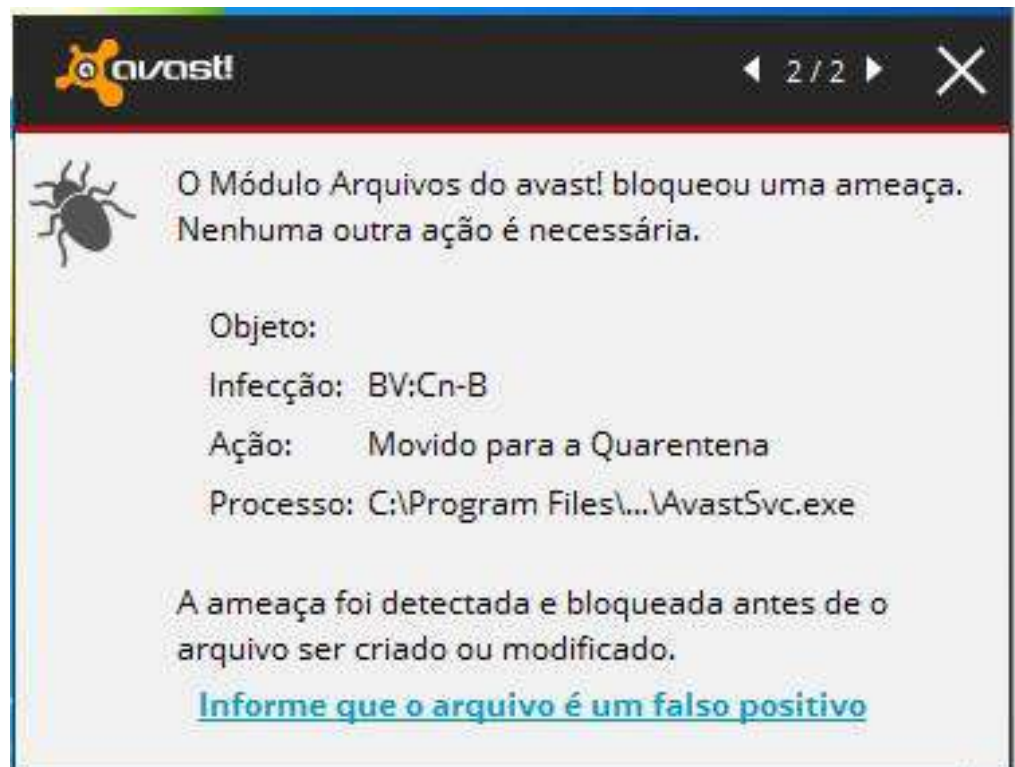


Figure 15 - In Portuguese, the Avast shows the message "The module Files of Avast! was blocked a Theat. No actions are necessary" free translation by the author.

7.3. Summary

The society is having loss much money, security, and tranquillity because security vendor does not dare to confront the reality. All systems are patched patchwork unsafe. A new generation must have the courage to redesign everything from scratch in the future, without patches. Also, society needs to teach security to students today so that that day can come true.

Security Systems chapter was presented methods to create a cyber autoimmune disease and scenarios analysis to use it over military thinking. It serves to alert governments and the military to previous protection and development of the active defence.

Antivirus systems are designed to combat threats that increase in complexity as the attack technologies have also evolved. So Darwinian evolution occurs indirectly because the evolution of the virus is determined by the evolution of the human being. This causes wondering about the effectiveness of the technology that is currently being applied to defend computers over the last 30 years. The ‘signature’ concept for malware detection probably stemmed from an analogy with the human immune system – as the antivirus defence system works similarly.

However, it is worth noticing that antivirus systems also analyse the behaviour of any given strange entity, aiming to identify it as something to be eliminated or not. From that, it’s plain to see that another mechanism – not just signature recognition – can be used to identify potential threats. An established model adopted by major manufacturers is transaction management (Oracle 2016) in the relational database

management system (RDBMS). In this model, an operation will receive a 'commit' after the operations that make up the process have been carried out successfully. Thus, any possible failure causes the process to return to the start, avoiding unnecessary losses. Currently, this method is only performed in the laboratories of antivirus companies, when designing their products.

Trust is broken when speech differs from the practice. This is particularly serious concerning cyber defence, potentially representing huge implications. The present research has demonstrated that the current commercially available antivirus software is being implemented using, for some particular kind of more complex attacks, inefficient methods.

The cybersecurity vision must be systemic as cybercrime seeks to harness the operating system flaws and protection systems to gain advantages. A security hole inserts mistrust and causes financial losses both for users and producers. A great competitive disadvantage can bring disastrous results for any company, and depending on the degree of exposure.

The next chapter explore the dilemma of cyber security education.

8. Cyber Security Education

8.1. Introduction

The previous chapters intent to demonstrate that software companies give credential management, security and privacy at a poor level. Many researchers will focus on the technological aspects of these cases, like program and project errors. Some people can study the environment implicit in the companies, and governments and others will point that the process can be corrupted. This chapter proposes a common point that links the problems presented in the early chapters.

In the chapter about Encryption, Privacy, Web Credential, and Security Systems this research explores how failures in programming and process can destroy efforts to keep secrets safe. The technology already promises quantum cryptography, but if the vendors and users continue to manage the credentials similarly to today, it is like a locked car with the key in the door's car.

This chapter explores the human factor and how UK Universities having taught about cyber security. Section 0 is presented a survey with the results of reading the curricula of a hundred UK Universities, specifically of G400 (Computer Science) courses. This work shows that cyber security is not so relevant for UK Universities when the author believes it is necessary.

To try to locate the universities that give more importance to Cyber Security education in the G400 courses, section 3.5.2 presents the proposal of an index that intends to rank universities according to the degree of importance given in their curricula for Cyber Security education.

8.2. Author's Contribution to Cyber Security Education

This chapter is based on o two publications:

A Study of the UK Undergraduate Computer Science Curriculum, 2019, London. IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019 (Ruiz, 2019);

The motivation to start this work was the perception that something in common could be at the origin of the problems verified and presented in most of the previous texts that I published. This work has examined a hundred computer science undergraduate courses in the UK, to assess the capability of the software developers in the Country to create secure pieces of software. Was evaluated to what extent the

UK Engineering and System Design students are being taught about the relevance of security issues when developing software. This theme is treated as just a voluntary element at the end of their professional education. Some of those principles are highly relevant to this work: Firstly, it is easier for students when they establish a firm foundation on Cyber Security before adding new knowledge.

- Individual contribution: Unique writer of the article.

Cyber Security Index For Undergraduate Computer Science Courses in the UK at the Journal of Applied Security Research, 2020. (Ruiz, et al., 2020)

This research proposes the creation of an index to classify UK Universities by the relevance that each institution teaches Cyber Security content. This work analyses the education of UK students who are responsible for developing software based on Cyber Security standards in G400 courses. Considering 100 UK universities to represent a relevant sampling in the universe of the UK. Inferring an easy 5 stars classification based on the index rating. The results display that 1 and 2 Stars represent 80% of the UK and 3, 4 or 5 stars was received just 20%. This work aims to raise awareness among British universities to pay more attention to teaching information security in computer science courses. Teach Cyber Security at the base is proposed by this research. It is better than most people know how to use a match than to train a large number of firefighters.

- Individual contribution: Principal writer, with the advisor of Dr. Pancham Shukla and Professor Hassan Kazemian

This work proposes a Cyber Security index that can demonstrate how Cyber Security is teaching in Computer Science (G400) courses in the UK (Ruiz, et al., 2020). The concern about Privacy Issues is closely linked to Cyber Security issues and (Ruiz, et al., 2020) explores these questions relating many studies involving privacy to the

educational system.

Society needs to rethink the grade for graduation degree courses for “System Analysis” and similar courses. After analysing the discipline grade of two principal’s courses of graduation degree in Brazil. The authors of UNICAMP (UNICAMP, 2017) and Federal Institute of São Paulo (IFSP, 2017), can’t find relevant hours that discipline that form the students to understand Cyber Security, physiology, sociology, discourse analysis, or other human factors disciplines for Cyber Security and consider that the focus is excessive in the technical aspects, UNICAMP course of Technology in Analysis and System Development has Zero hours of Cyber Security specific discipline and has 30 hours of Society and Technology discipline. (Silva, 2012)

Brazilian Federal Institute of Education (Prof. Alencar de Melo Júnior, 2017) has 80 hours of Cyber Security (in the last semester) in his course of Analysis and System Development graduation degree. Few hours of safety content being taught at the end of the course causes a major learning problem. The student learns to develop systems during years without specific orientation about secure programming.

8.3. Summary

Studying how Cyber Security is offered to computer science students in the UK by reading the subject and content grades provided by a hundred British universities has co-confirmed suspicions raised since the beginning of the first published article that made up this thesis. This chapter provides a critical survey of cyber security education status in UK Universities and provides a method to classify how relevant is cyber security in this environment.

The data presented demonstrate that teaching Cyber Security content is flawed in the UK. Offering these subjects as a subject and optional content at the end of the course would be the equivalent of providing children broccoli after they have had lunch and eat dessert ice cream. It is very important, but the order and manner of the offer are completely wrong according to common sense that society applies to their children in basic teachings and according to the most renowned educators' neuroscience and guidelines.

It is not reasonable to expect quality and efficiency in software security requirements when students are encouraged to despise these contents. Only a few interested in specializing in the field attend these classes and, in general, are already looking for specialized courses to train Cyber Security specialists.

It is important to emphasize that this study intends to demonstrate the need for all know about Cyber Security, whether as mere users, as specialists, or mainly in this study's focus as software developers.

Trying to change this reality, this study offers the community an evaluation index that can indicate the universities most committed to a curriculum rich in Cyber Security, able to return to society, less vulnerable software and mainly a culture of security and privacy instilled in the habits of their students that will be disseminated throughout British society. After discussing these five security elements, the conclusion is presented below.

9. Discussion

This is a thesis by compendium of previous publication, “prior publication way”. Because of the large number of published work included in this thesis, the entire thesis was divided in five elements of cyber security. This section presents Discussion of Findings and the Implications, and Limitations of the thesis in five subsections of discussion, one for each element: Privacy, Encryption, Web Credentials, Security Systems and Cyber Security Education.

9.1. Privacy

After the tests using the proposed method, it can return to the issues that gave rise to the current chapter. Can the data acquisition method used for testing be considered efficient for evaluating privacy aspects? The answer is yes, and the method is being used and cited by other authors. Can privacy be guaranteed when the browsers are used in private mode? The answer is not, according to the results presented in Table 9. A sample of image and code recovered can be found in Figure 16 and Figure 17. In

Figure 16 is possible to see the page visited during the private mode and Figure 17 show that after private navigation, the entire code of visited page was recovered.

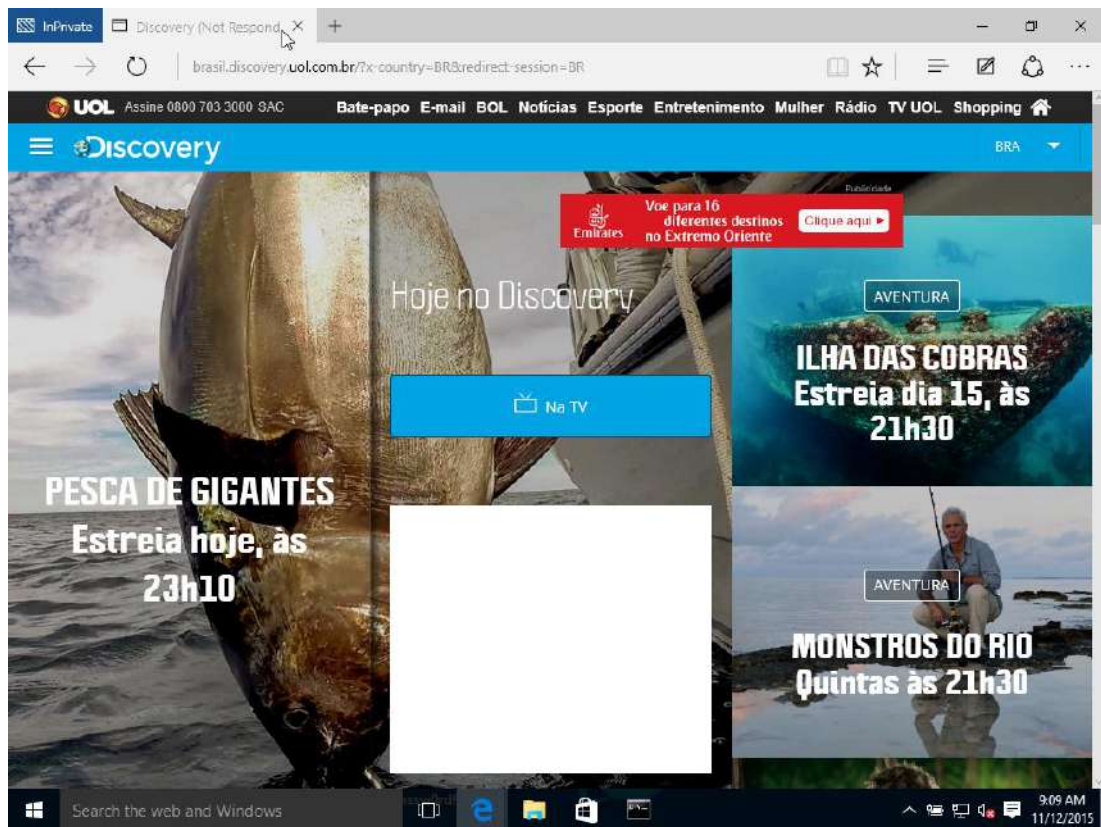


Figure 16 - Discovery Channel web page accessed with Windows Edge in private mode navigation.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
OBODED80	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
OBODED90	20	20	20	20	20	20	20	20	09	3C	73	65	63	74	69	6F	<sectio
OBODEDA0	6E	20	63	6C	61	73	73	3D	22	66	65	61	74	75	72	65	n class="feature
OBODEDB0	64	2D	69	74	65	6D	2D	73	74	79	6C	65	2D	31	22	3E	d-item-style-1">
OBODEDC0	0D	0A	09	09	20	20	20	20	20	20	20	20	20	09	09	3C	<
OBODEDD0	66	69	67	75	72	65	20	63	6C	61	73	73	3D	22	69	74	figure class="it
OBODEDE0	65	6D	22	3E	0D	0A	20	20	20	20	20	20	20	20	20	20	em">
OBODEDF0	20	20	3C	64	69	76	20	63	6C	61	73	73	3D	22	69	6D	<div class="im
OBODEE00	61	67	65	46	69	72	73	74	22	3E	0D	0A	20	20	20	20	ageFirst">
OBODEE10	20	20	20	20	20	20	20	20	20	3C	69	6D	67	20	64	61	<img da
OBODEE20	74	61	2D	73	72	63	3D	27	68	74	74	70	3A	2F	2F	72	ta-src='http://r
OBODEE30	65	73	2E	63	6C	6F	75	64	69	6E	61	72	79	2E	63	6F	es.cloudinary.co
OBODEE40	6D	2F	64	62	37	39	63	65	63	67	71	2F	69	6D	61	67	m/db79cecgq/imag
OBODEE50	65	2F	75	70	6C	6F	61	64	2F	63	5F	63	72	6F	70	2C	e/upload/c_crop,
OBODEE60	68	5F	38	39	39	2C	77	5F	31	31	39	39	2C	78	5F	31	h_899,w_1199,x_1
OBODEE70	31	38	2F	63	5F	66	69	6C	6C	2C	68	5F	33	39	30	2C	18/c_fill,h_390,
OBODEE80	77	5F	35	32	30	2F	76	31	34	34	36	36	35	39	36	33	w_520/v144665963
OBODEE90	31	2F	69	6C	68	61	2D	64	61	73	2D	63	6F	62	72	61	1/ilha-das-cobra
OBODEEA0	73	2D	63	6F	76	65	72	2D	79	2E	6A	70	67	27	20	61	s-cover-y.jpg' a
OBODEEB0	6C	74	3D	27	69	6C	68	61	2D	64	61	73	2D	63	6F	62	lt='ilha-das-cob
OBODEEC0	72	61	73	2D	63	6F	76	65	72	2D	79	27	20	20	77	69	ras-cover-y' wi
OBODEED0	64	74	68	3D	27	35	32	30	27	20	20	68	65	69	67	68	dth='520' heigh
OBODEEE0	74	3D	27	33	39	30	27	20	2F	3E	20	20	20	20	20	20	t='390' />
OBODEEF0	20	20	20	20	20	20	20	3C	2F	64	69	76	3E	0D	0A	20	</div>
OBODEF00	20	20	20	20	20	20	20	20	20	20	20	20	3C	64	69	76	<div
OBODEF10	20	63	6C	61	73	73	3D	22	69	6D	61	67	65	53	65	63	class="imageSec
OBODEF20	6F	6E	64	22	3E	0D	0A	20	20	20	20	20	20	20	20	20	ond">
OBODEF30	20	20	20	20	3C	69	6D	67	20	64	61	74	61	2D	73	72	<img data-sr
OBODEF40	63	3D	27	68	74	74	70	3A	2F	2F	72	65	73	2E	63	6C	c='http://res.cl
OBODEF50	6F	75	64	69	6E	61	72	79	2F	63	6F	6D	2F	64	62	37	oudinary.com/db7

Figure 17 - Data recovered after a system reboot. All data on the Discovery Channel web page was recovered.

In this context, this research discusses two possibilities of responsibility: the effects of the operating system in private mode browsing and the functionality itself in the browsers. Inside the first case, the software is constructed upon the working device abstraction layers, and numerous functions and device calls required for browsers are imported from the operational device itself. In this way, memory control and i/o operations are below the operational gadget domain, disposing of the browser's power to determine what ought to be recorded and wherein on. Without complete manipulation of these moves, the browser depends on the os to hold the consumer's privacy.

Inside the second case, the browser's area, the developer creates an expectation of privacy in users after they claim that their software program has functions that might

prevent others from reconstructing the stairs the users took all through their online activities. For example, Firefox and tor package browsers rely upon unique features to the home windows working machine.

But, with the opportunity of user's privacy loss, as shown in the effects accrued on this work, the builders' statements about the insurance of consumer's privacy appear misleading and, consequently, can induce the users to mistakes.

Then again, in the IE, chrome, and safari browsers, builders are the same builders of the operational system. Because of this, the builders have a situation to control and change the machine conduct. However, what as seeing is a situation just like that included in the preceding paragraph. Even in favourable conditions, browsers conduct is equal, leaving residues that would allow a few forms of the identity of customers' web browsing habits. The present research about private mode browser functionality demonstrates that "*InPrivate*" or "*Incognito*" navigation is not sufficient to guarantee users' privacy when tested with the proposed method and boundary conditions.

The method used to collect and analyse the data is valid to evaluate the implementation aspects of private browsing. It permits the build of a privacy model that supported the discussions and elucidated the key elements analysed that ultimately presented problems in implementing various browsers' private-browsing functions and operational systems' resources.

Concluding, it is possible to verify that all browsers tested presented flaws in their private browsing mode.

Those flaws permit data that remain available in the system and expose not only the identification of pages visited but, in some cases, also allows to partially or

rebuild them.

Vendors promise to leave no traces of the navigation activities of users. This work shows that privacy, as advertised, is not provided.

As a final recommendation, this research suggests the developers explicitly alert the users about the limitations of the private browsing functionality implementation. “We need to teach about privacy importance since the first day of class.” (Ruiz, et al., 2020)

This method is limited by the versions of browsers analysed.

9.2. Encryption

The exploration of failures in credential management used in the most famous and prestigious encryption software available in the global market was the core of all Encryption section. For this, it was provided three methods to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods. It is relevant to use in crime labs that investigate suspicious activities encrypted in the suspect hard drive.

In the Cyber Security, are "Ten Immutable Laws of Security" according to (Microsoft Corp., s.d.) and some of these laws can be discussed.

“Law #1: If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore”;

“Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore”;

“Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore”;

“Law #4: If you allow a bad guy to run active content on your website, it's not your website any more”;

“Law #5: Weak passwords trump strong security”;

“Law #6: A computer is only as secure as the administrator is trustworthy”;

“Law #7: Encrypted data is only as secure as its decryption key”;

“Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all”;

“Law #9: Absolute anonymity is not practically achievable, online or offline”;

“Law #10: Technology is not a panacea”.

Microsoft BitLocker was flagging off the security system with a feeble recovery password equal regardless of the change of password. This is inconsistent with Law #7 because a weakened password gives a higher probability of success to an attacker. Likewise, additional time was detected when Law #5 was cracked because developers intentionally create a much weaker recovery key (section 6). Similar state occurred Security weaknesses LM hash (Sanders, 2010), when the weakening password enabled attacks with great effectiveness with breakable protection. BusinessWeek in January 2011 shows among other information that about 30% of help desk calls refer to resetting keywords (Bloomberg Business, 2011).

Encryption software is deployed insecurely. The main differences between the information presented during the process of sale and the security of the product concerning what the user will receive. The management of identities and passwords is

not secure. Microsoft created its “Ten Immutable Laws of Security” to clarify users of the need to take care of information security. When “Ten Immutable Laws of Security” are compared with BitLocker, does Microsoft advertising hurt some of its laws?

Beyond software problems, it is visible problems in the environment, process, and people training. Universities (University of Michigan, 2018) (Wake Forest University, 2014) (Wake Forest University School of Business, 2018) define unsafe process sharing passwords of crypto containers and induce the researchers and students to create unsafe memories that will be used in other kinds of software and processes in their lives.

Billionaires’ industry and government secrets are unsafe too when the process is transported from the university experiences for companies where university students are working and will be future collaborators. There is a direct link between the way students are trained and the safety of systems and that directly affects society's whole.

For a biochemistry student, the effect of a loss of sensitive data can affect himself or his company (Smith, 2003). Nevertheless, the effects of a computer science student's low and inadequate training in the safe use and safe programming techniques can have damaging effects in all areas of knowledge. These professionals create the tools used by all other areas of society, significantly raising their responsibility. It is possible to trace a parallel with the pandemic of COVID-19 closing schools published by OECD in September 2020. The conclusion of the report is that the student is not exposed to the appropriate content. The losses are great for the student and also for society that loses with their lack of training. (Hanushek & Woessmann, 2020).

This research does not discuss excellent mathematical algorithms. It focuses on identifying and exploring programming flaws in the management of the credentials

necessary to use these mathematical algorithms as shown in chapters 3.2.1, 3.2.2 and 3.2.3. In summary, this work does not break into the safe; it simply uses techniques to locate where the user keeps the keys. Published articles (Winter & Ruiz, 2016) (Ruiz, et al., 2014) (Rodrigo Ruiz, 2017) demonstrate that this has been done with considerable success.

This section was provided three methods to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods. It is relevant to use in crime labs that investigate suspicious activities encrypted in the suspect hard drive. In the next chapter the web credential management is explored. This work is limited to the versions of software tested and the human behaviours.

The result was the ability to open encrypted files using the old password protected by famous software. Access to new data was allowed using the password stored in the old file header. The user can change the password infinite times, and the old password will still open the new files.

9.3. Security Systems

The main similarity is the use of signatures, but the human immune system uses very complex processes. As an example of intruder detection, it is possible to observe the activities of T cells. As possible to identify these similarities seen in Figure 18 and Figure 19.

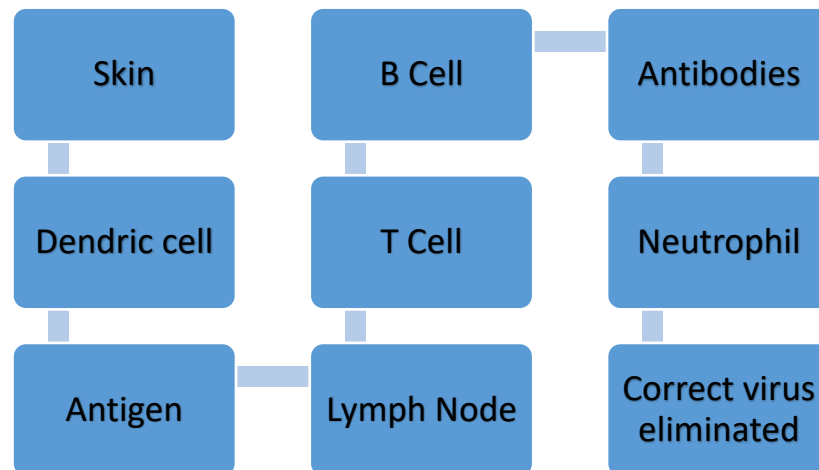


Figure 18 - Human system of protection resume. (Ruiz, et al., 2015)

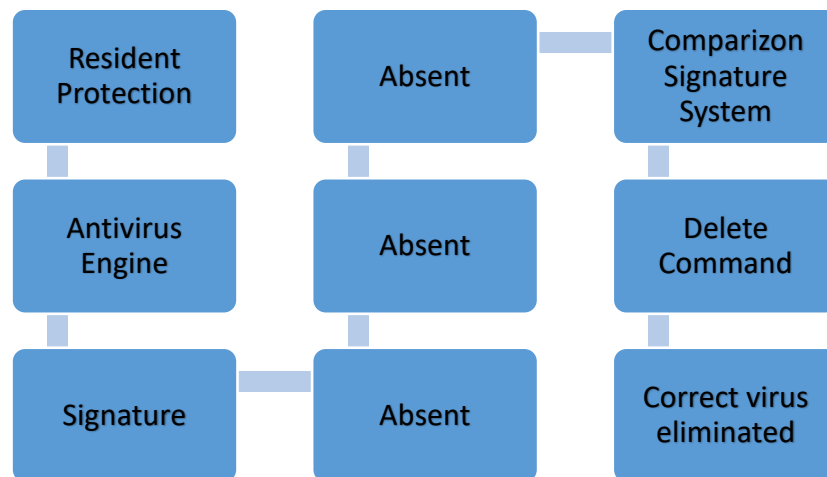


Figure 19 - Correlation of human protection system with cyber protection system. (Ruiz, et al., 2015)




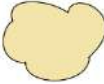
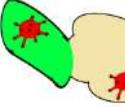
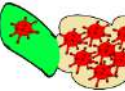
All antivirus system uses a signature system to identify a threat; the heuristics are just used at the vendor's lab to produce the signature⁵. In Table 11 is possible to understand each action of the antivirus system when exposed to the Apoc@lypse method and the results. It shows the action of antimalware in each situation and analyses if this action is correct or wrong.

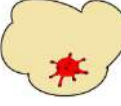
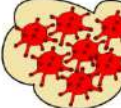
“The big problem of antivirus is the wrong use of the signature concept to distinguish between malicious and benign files. Thus,

⁵ Signatures are sequences of codes of varied sizes that identify one or more malicious archives, something that seemed a good idea up to the arrival of Apoc@lypse. A signature might be a sequence of codes in computer language. “9B 37???? 57 83 CD.” Another code might be any sequence of the type “IAMACOMPUTERVIRUS.” (Ruiz, et al., 2015)

with this kind type of classification, the antivirus system defines the actions that it will execute, such as clean, erase the file, or do nothing.” (Ruiz, et al., 2015)

Table 11 Apoc@lypse method, a sequence of events: an antivirus action.

Element/ action	Biological name	Cyber Equivalence	Antivirus action: to remove or to do nothing	The attitude of the antivirus: right or wrong
	Virus	Malware	Remove	Correct
	Harmless bacterium type lactobacillus	Commands archive in share BAT	Let go	Correct
	Bacterium infected to transport DNA of a virus	Commands archive BAT that is transporting malicious code	Let go	Wrong
	Host	Any lawful program used for transport of the bacterium BAT	Let go	Correct
	Infected host	A program that overdoes when BAT built in the code of a bacterium infected with virus DNA	Let go	Wrong
	Healthy cell	An archive of the user, programs, or operating system	Let go	Correct
	Bacterium transmitting the DNA of the virus for the cell in a way not invasive	Commands archive BAT that is being executed and writing the code of the virus at the end of an archive of the user or the system	Let go	Wrong
	Bacterium transmitting the DNA of the virus for the cell in an invasive way	Commands archive BAT that is being executed and substituting completely the code of the archive for that of the virus in the interior of an archive of the user, or of the system	Let go	Wrong

	A cell infected with the virus in a noninvasive way	An archive of the user, programs, or operating system that had the code of the virus annexed to the end of the archive	Remove	Wrong
	A cell infected with the virus in an invasive way	An archive of the user or operating system that had his content completely substituted by the code of the virus	Remove	Correct

This kind of Cyber Security problem can be used in commercial competition and as a military weapon. (Ruiz, et al., 2015) (Rogerio Winter et al., 2020) (Ruiz & Winter, 2015) (Winter & Ruiz, 2017) (Winter & Ruiz, 2016)

60% of US small businesses that suffer some type of cybercrime go bankrupt within six months. (Miller, 2016) The term “Cyber autoimmune disease” (Ruiz, et al., 2015) indicates, and the tests were demonstrated that the core of antivirus is just a slot machine. Table 12 as possible to verify the impact in some G20 nations.

Table 12 Spent on Cybercrime as a Percentage of the GDP (Source: Intel Security Studies, 2014))

Country	% of GDP	Confidence *	G20	PIB (billion US\$)
Australia	0.08%	M	X	1530
Brazil	0.32%	M	X	2240
Canada	0.17%	M	X	1826
China	0.63%	M	X	9240
France	0.11%	L	X	2806
Germany	1.60%	H	X	3730
India	0.21%	L	X	1876
Italy	0.04%	L		2149
Japan	0.02%	L	X	4919
Russia	0.10%	M	X	2096
United Kingdom	0.16%	L	X	2678
United States	0.64%	H	X	16768

* Label: L = Low, M = Medium and H = High

As a cyber weapon or tool for antivirus industry improvement, the Apoc@lypse

technique is the first proof of cyber autoimmune disease. The limitation of this method is the use of signature systems and the damage is much more intense in the Windows systems in the tested versions.

9.4. Web Credentials

During the tests, the private browsing function was turned on. The InPrivate or incognito mode was activated in Internet Explorer's "InPrivate", Firefox's "Private Browsing", Chrome's "Incognito", Safari's "Private Browsing", Opera's "Private Browsing" and Robot "Incognito" functions. TOR Browser comes with default private browsing.

In (CARRIER, 2005) data analysis technique is essential and seeks information in byte or sector address of the data unit is called by (CARRIER, 2002) Data Unit Viewing.

Signatures are the other way to find a data proceeding search with Logical File System Level Searching.

This study chose the Logical File System Level Searching and started looking for pardons and creating signatures. Digital Forensic tools for data carving (Foremost, s.d.) and (WinHex, s.d.) were used to search for information related to credentials.

To create each signature as seen in Table 5, this research has opened the disk image with WinHex and a search for a unique and easy identifiable password earlier defined and used to log on to the site tested. Only in Internet Explorer's case, the following directories and files contained the recovered information about authentication:

`\users\user\appdata\local\microsoft\internet Explorer\recovery\last active\`

internet

\users\usuário\appdata\local\microsoft\windows\temporary
files\low\content.ie5\

\Pagefile.sys

It is possible to visualize four levels of responsibility: Operating System, Web Browser, Frameworks, and Web developer. The OS ought to be modified to use cryptographic features to control the switch memory. The Web Browser operations having a conscience about the OS vulnerability and need to be modified to protect the user.

Frameworks must be changed to allow the login and password fields to be secured with encryption and to save the user's credentials.

Most important, web developers need to consider Cyber Security in the First Line of code and provide solutions to fix OS, Browser, and Framework problems, imputing a secure code into the program.

Today some big companies like Google, Microsoft, LinkedIn, Facebook, and many others have offered the service to provide authentication (Google, s.d.). This kind of service is used in an attempt to disclaim the responsibility for maintaining and storing user credentials using the name and credibility of an internet giant. But this method succumbs to the one proposed in this work where some of these companies have been tested and failed. No matter where the authentication takes place, everything that is typed on the client's computer is recorded on the client's computer in clear text. Remember that the same companies that offer the authentication services, failed to provide privacy in the credentials of their products.

9.5. Cyber Security Education

9.5.1. Cyber Security Education in UK

Computer Science Courses

The analysis obtained from the obtained science and the tabulation of the contents, and the reading presented to the students of Computer Science courses in the UK leaves little importance for cybersecurity, at least formally.

While Figure 20 shows that 39% of G400 in UK Universities still have no mandatory Cyber Security content.

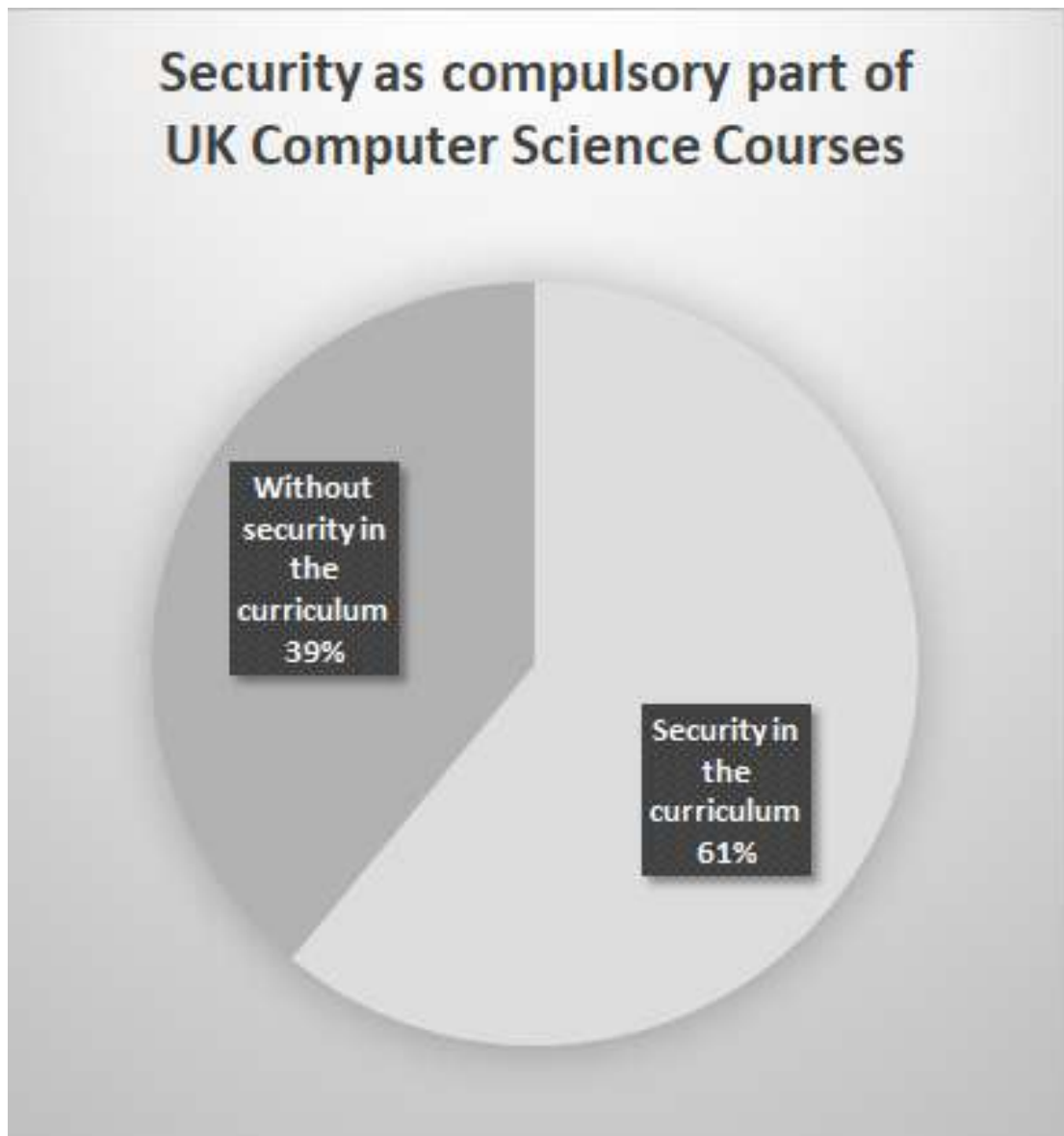


Figure 20 Considering 100 Computer Science Courses, Security as an optional discipline or an element of other disciplines on the UK computer science courses. 61% have security on the curriculum and 39% have no security on the curriculum. (Ruiz, 2019)

Figure 21 considers the total contents 189 under 100 G400 to demonstrate that 54% of courses have mandatory Cyber Security elements on the curriculum and 40% have optional security content.

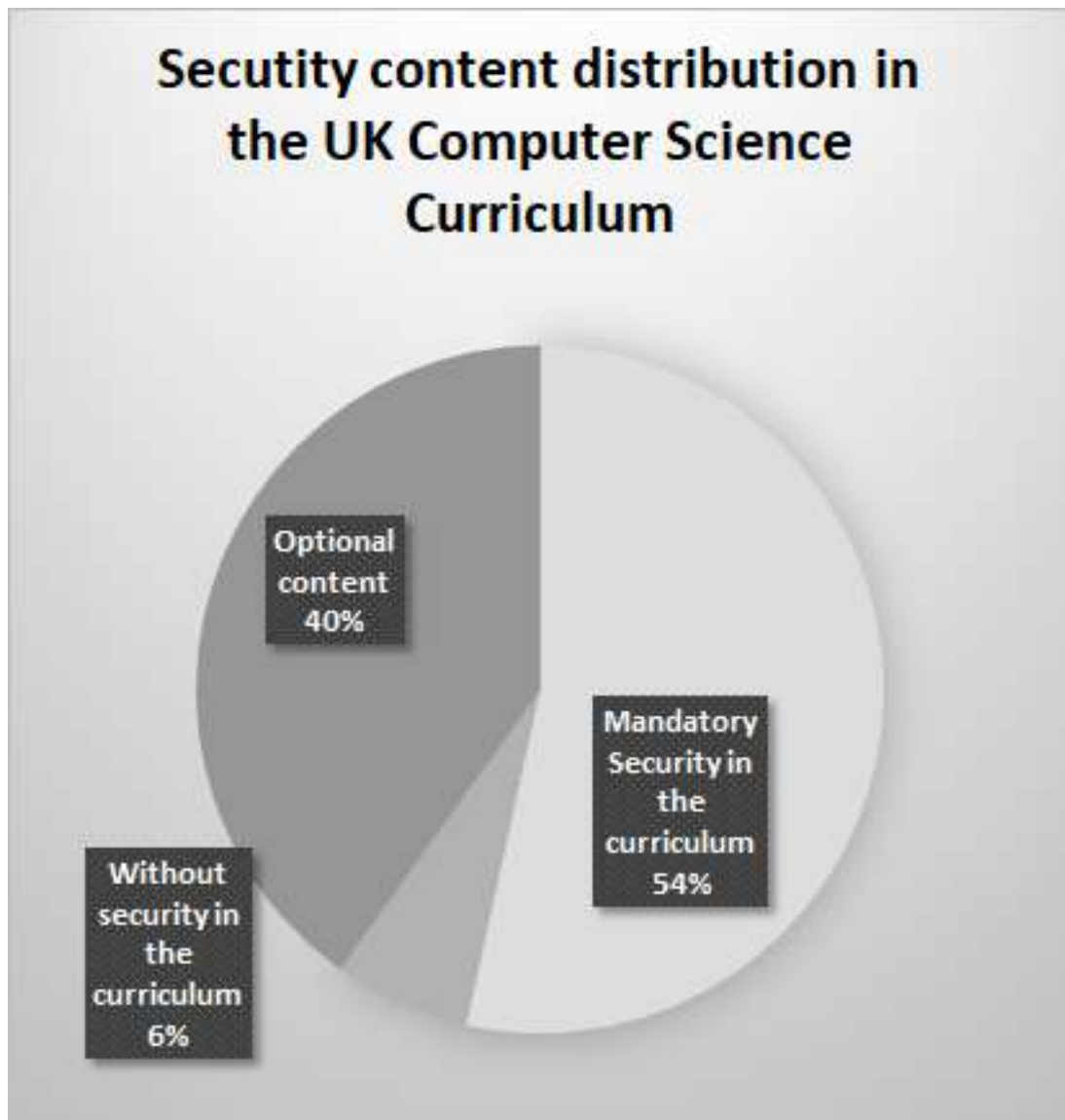


Figure 21 Considering the total contents 189 under 100 Computer Science Courses, Security as a mandatory discipline or an element of other disciplines on UK computer science courses. 6% of courses have no security content on the curriculum and 54% of courses have mandatory Cyber Security elements on the curriculum and 40% have optional security content. (Ruiz, 2019)

Finally, Figure 22 shows that 60% of Cyber Security content is concentrated in the third year or later.

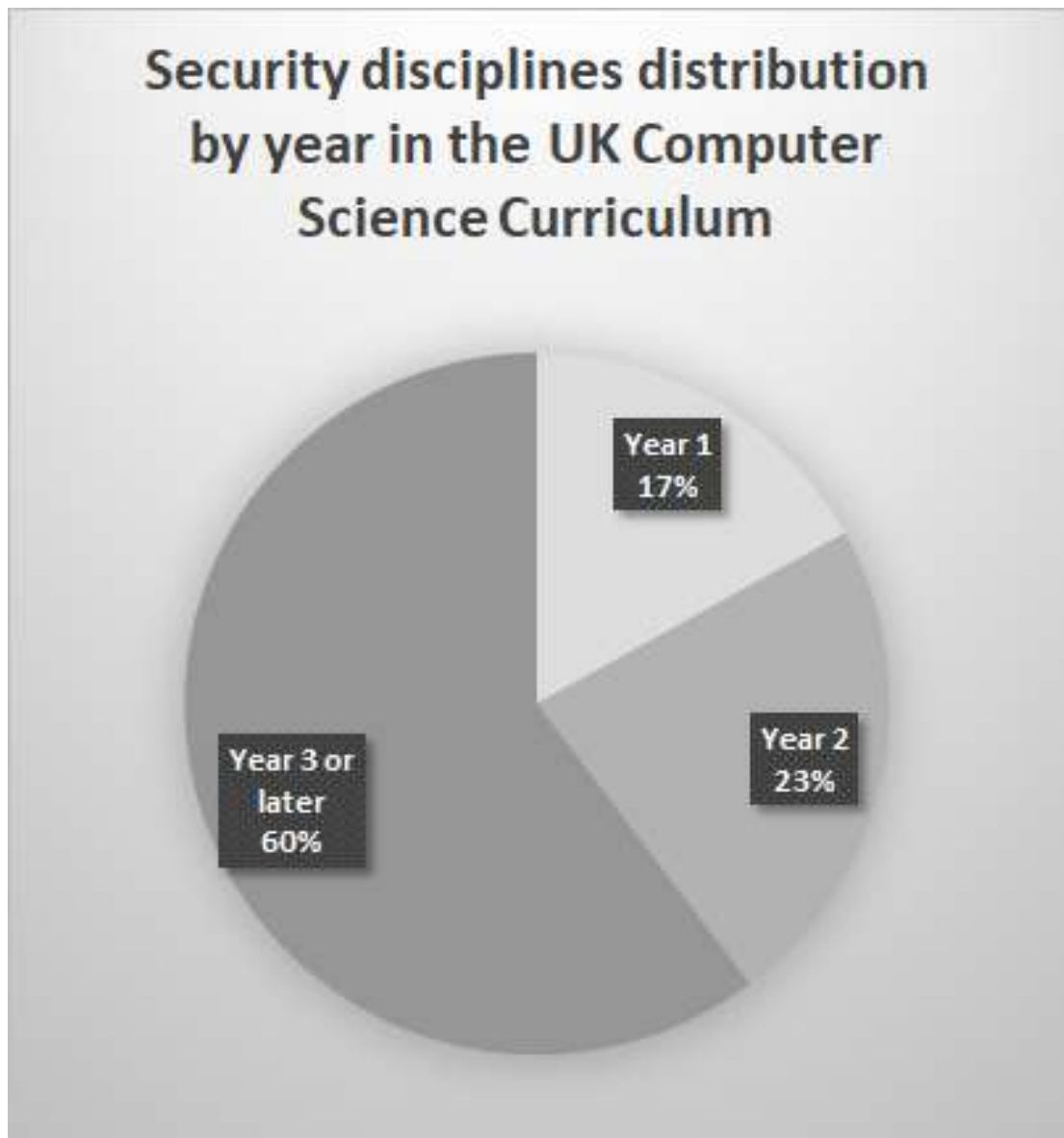


Figure 22 Considering the total 189 security content, Security discipline's distribution by year on UK computer science courses. 17% focus on security content in the first year, 23% in the second year, 60% in the third year or later. (Ruiz, 2019)

To teach about Cyber Security at the end of the course and leave this kind of content as optional is the biggest problem that this section likes to expose. The first stage in the process of acquiring knowledge is to “remember” (Bloom, 1956). Important to verify that UK students are not being exposed to Cyber Security since the beginning. According to (Chrysikos, et al., 2017), UK students of computer science undergraduate prefer to be explicitly identified about content expectations and instructors so that to support them in a laboratory. How does it about Cyber Security

if this content is not explicit on curricula?

9.5.2. IRCS (Index of Relevance in Cyber Security)

Table 8 provides a list of 100 UK Universities that offer G400 or very similar courses. Column (a) show the UK ranking, (b) World Ranking according to (Cybermetrics, 2018); (c)IRCS (Index of Relevance in Cyber Security), (d) University; (e) Total of Cyber Security content; (f) Total of Cyber Security content taught as optional; (g) Total of mandatory Cyber Security content; (h) Total of Cyber Security content in the first year; (i) Total of Cyber Security content in the second year; (j) Total of Cyber Security content in the third year; (k) Total of Cyber Security content in the fourth year; (l) Total of Cyber Security content in the fifth year; (m) Total of Cyber Security content in the sum of last 3 years.

The propose of (Nance, et al., 2012) teaches Cyber Security early, into k-12 courses in the US also (Taylor & Azadegan, 2005) are developing a prototype of curricula into Computer Science course at Towson University to improve Cyber Security content and (Yue, 2016) more specifically propose that Cyber Security researchers consult with the instructors of non-security courses, identify the relevant Cyber Security topics, and discuss the corresponding topics in the classes.

If a 5-star classification as seen in Table 8 are inferred, using the IRCS index like this (1 Star IRCS <1 , 2 Stars IRCS between 1 to 1,99, 3 Stars IRCS between 2 to 2,99, 4 Stars IRCS between 3 to 3,99 and 5 Stars IRCS ≥ 4). This data was extracted, in the UK with 2019 according to (Ruiz, et al., 2020):

1 Star represents 54% of UK selected courses;

2 Stars represent 26% of UK selected courses;

3 Stars represent 11% of UK selected courses;

4 Stars represent 6% of UK selected courses;

5 Stars represent 3% of UK selected courses.

This research concludes that universities need to improve more Cyber Security into G400 courses in the UK as an alternative to improve more quality in software and turn Cyber Security safer for all society.

The limitation of this work is the official content of UK Universities Curriculum.

10. Conclusion

As a Global concern, cyber security will define how ease will be the modern human life. This work has been actual for a decade and a substantial set of Cyber Security publications was presented, discussed, and analysed in Privacy, Encryption, Web Credentials, Security Systems, and Education. Offering ten methods to improve Digital Forensics arsenal.

These contributions are published in a series of fifteen research papers at: The Seventh International Conference on Forensic Computer Science - ICOFCS 2012, Brasilia, Brazil; At Proceedings of the International Conference on Information Security and Cyber Forensics, 2014 Kuala Terengganu, Malaysia; At International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2015; At Science Magazine, 2020; at The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014), 2014, Kuala Lumpur, Malaysia; At Cyber Security Review Magazine, 2016; at Journal of Cyber Security and Mobility, 2016; At Journal

of Payments Strategy & Systems, 2017; In a book published in 2015 indexed by ACM; at Cyber Defence Magazine, 2015; At Cyber Security Review Magazine, 2016; at Critical Infrastructure Protection Review Magazine, 2017; At International Journal of Cyber-Security and Digital Forensics, 2107; At IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019; at Journal of Applied Security Research, 2020 and at 22 nd European Conference on Knowledge Management ECKM, Coventry University, 2021, Fully presented in Appendix U

On **Privacy**, this works was present three versions of the method to restore *in private* or *incognito* mode navigation, able to expose all navigation made over *incognito* mode. The method works over browsers like IE, Edge, Firefox, Safari, Chrome, Opera and TOR over Windows systems. The generic method of collection and analysis contributed significantly to the given conclusions about the limits of the private browsing functionality. Moreover, it permits to analyse and identify possible flaws in the chain of privacy, from aspects ranging to the knowledge collected by the operating system through the implementation and use of the private browsing mode in modern browsers. It is relevant to use in crime labs that investigate suspicious activities in the suspect machine.

About **Encryption** this research was provided three methods to bypass cryptographic systems to gain access to the encrypted files. Symantec Encryption Desktop, BitDefender Total Encryption and Truecrypt variants are covered by these methods. This work was tested famous encryption software and identified a vulnerability that permits information leakage. The guiding principles behind information security are summed up in the acronym CIA, standing for Confidentiality, Integrity and Availability. People want the information to be read by only the right people, only be changed by authorised people or processes and, be available to read

and use whenever necessary. As a solution aiming at keeping secrets – protection against cybercriminals, the user acquires cybersecurity solutions software & hardware, since any loss or leakage of information may cause serious damages such as reputation, financial losses etc. It is relevant to use in crime labs that investigate suspicious activities encrypted in the suspect hard drive.

Web Credentials chapter was explored how to get clear text credentials after the analyst having access to the computer target. The proposed method can get credentials used in intranets or e-commerce, home banking and email accounts. To minimize the problem the operating system must be changed to use cryptographic features to manage the swap memory. In this way, if a computer is inadvertently shut down, the user information will be saved and will not be recovered even with forensic operations. Web browser operations need to be modified to protect the user because the operating system stores data on the hard drive without proper security handling. Finally, web developers should consider security by design and review all site building codes and processes. All web system components must be tested to prevent failures and keep user data safe. It can be used in criminal investigations or to improve more strong security in these websites.

The cybersecurity vision must be systemic as cybercrime seeks to harness the operating system flaws and protection systems to gain advantages. In the chapter, **Security Systems** this work was presented methods to create a cyber autoimmune disease and scenarios analysis to use it over military thinking. A security hole inserts mistrust and causes financial losses both for users and producers. Antimalware software shows that technical applications can be wrong and thus a complex technology is used to translate the behaviour of a threat in a simple signature so that we understand how relevant a change in the paradigm is. The heuristic system must be

implemented on the client machine and enable-threatening movements of malware are contained in the first steps. It serves to alert governments and military to previous protection and development of the active defence.

There is no point in continuing to create more and more courses for cybersecurity experts. Today, these professionals are involved in repairing programs with little notion of cybersecurity. In the meantime, education and training are the more accessible ways to prevent and fix cybersecurity problems. About **Cyber Security Education**, this research provides a critical survey of cyber security education status in UK Universities and provide a method to classify how relevant is cyber security in this environment.

Also, this work presents in Appendix A, the metrics of academic contributions, listing the citation. A Novel Approaches to Applied Cyber Security in Privacy, Encryption, Security Systems, Web Credentials, and Education contributes significantly to the academy in the field of cybersecurity, analysing scenarios and sensitive issues in the daily life of the digital society and proposing methods for improving global cybersecurity.

11. Future Work

Active defence is a concept that is distributed worldwide among military and intelligence officers. This project seeks to present solutions for active defence in the management of credentials and access to critical systems with the main objective of safeguarding human lives and avoiding conflicts.

The military having the most powerful computers and systems and it needs to be safe and protected. Continuous assessment of operating systems, browsers and cryptographic programs have already generated many security disclosures about breaches and failures found in (Aggarwal, Bursztein, Jackson, & Boneh, 2010) and (Carrier, File System Forensic Analysis, 2005).

The present research project focus on the treatment of a user's login information (usernames and passwords) by important military websites that provide internal services. The data gathered and treated gave important details about how those sites manage their user's passwords on the client side. Military forces having

thousands of equipment's and persons produces a scenario to stolen hardware and data.

A method to gain credentials in commercial websites was published by (Ruiz, Winter, Park, & Amatte, 2017). This project will adapt and use this method to explore military websites vulnerabilities. With user and password is possible to having access to sensible data. This project wants to evaluate military vulnerability over the internet using the previous method developed by the author using forensic techniques.

No device or system will be hacked or improperly accessed in this project. The simple fact of entering the publicly available address available and disclosed by the owner of the website causes this website to record unsolicited data on the user's computer, in this case, the analyst computer.

References

- E. DENNING, D., 1987. An Intrusion-Detection Model. *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, FEBRUARY, pp. 222 - 232.
- ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, 2017. *Cybersecurity Curricula 2017*, New York: ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8.
- ACM, 2020. *Association for Computing Machinery*. [Online]
Available at: <https://www.acm.org/>
[Accessed 03 03 2020].
- Acunetix, 2019. *Web Application Vulnerability Report*, s.l.: s.n.
- AGGARVAL, BURSZTEIN, G., JACKSON, E. & BONEH, C., 2010. *An Analysis of Private Browsing Modes in Modern Browsers*. s.l., s.n.
- Aggarwal, G., Bursztein, E., Jackson, C. & Boneh, D., 2010. *An Analysis of Private Browsing Modes in Modern Browsers*. Washington, DC, s.n.
- Ahmad, M., Idris, M., Pervez, Z. & Lee, S., 2015. *Vulnerability Analysis for Credentials Management in Web Browsers*. Seoul, The international conference on Future Web.
- AJ Willingham, CNN, 2019. *The family of a teen who died by suicide after being outed by cyberbullies is demanding justice*. [Online]
Available at: <https://edition.cnn.com/2019/09/30/us/channing-smith-suicide-cyberbullying-tennessee-trnd/index.html>
[Accessed 20 05 2020].
- Alexandron, G., Armoni, M., Gordon, M. & Harel, D., 2017. Teaching Scenario-based Programming: An Additional Paradigm for the High School Computer Science Curriculum, Part 1. *Computing in Science & Engineering*, 19(5), pp. 58-67.
- Andress, A., 2013. Integrating People, Process and Technology. In: *Surviving Security*. s.l.:s.n.
- Anon., 2020. *IEOM Brazil 2020*. [Online]
Available at: <http://ieomsociety.org/brazil2020/committee/>
[Accessed 23 03 2020].
- Anti-Malware-Test.com, 2012. *ANTI-MALWARE TEST Tests Methodologies*. [Online]
Available at: <http://www.anti-malware-test.com/node/198>
[Accessed 19 07 2020].
- Apple Inc., 2014. *Defending your online privacy and security*. [Online]
Available at: <http://www.apple.com/safari/>
[Accessed 15 November 2014].
- AV COMPARATIVES, 2014. *AV COMPARATIVES File Detection Tests*. [Online]
Available at: <https://www.av-comparatives.org/tests/file-detection-test-september-2014/>
[Accessed 19 07 2020].
- AV Test, 2014. *AV Test - Test Procedures*. The Independent IT- Security Institute. [Online]
Available at: <https://www.av-test.org/en/about-the-institute/test-procedures/>
[Accessed 19 07 2020].
- Bai, L. et al., 2019. The Software Gene-Based Test Set Automatic Generation Framework for Antivirus Software. *JSW*, 4(10), pp. 449-456.

- Baker, J., 2018. Forgotten heroes of the Enigma story. *Nature*, pp. 307-308.
- Balcao, A. F. et al., 2019. *A Consumer-centric Conceptual Framework for Trust Assessment in Cloud Computing*. Abu Dhabi, s.n.
- Balcao, A. F. et al., 2020. *A study on Trust Models in Cloud Computing*. Las Vegas, s.n.
- Barabanov, A. V., Markov, A. S. & Tsirlov, V. L., 2018. Statistics of software vulnerability detection in certification. *J. Phys.: Conf. Ser. 1015 042033*, pp. 1-8.
- Bell, T., Andreae, P. & Lambert, L., 2010. *Computer Science in New Zealand High Schools*. Brisbane, Proceedings of the -12th Australasian Computing Education Conference(ACE2010).
- Bishop, M., 1997. *The State of INFOSEC Education in Academia: Present and Future Directions*. s.l., In Proceedings of the National Colloquium on Information System Security Education, pp. 19-33.
- Bishop, M., 2000. Education in Information Security. *IEEE Concurrency* 8(4), 10, pp. 4-8.
- Bishop, M. & al., (., 2019. Learning Principles and the Secure Programming Clinic. In: W. 1. L. P. J. 2. 2. P. 12th IFIP WG 11.8 World Conference, ed. *Information Security Education. Education in Proactive Information Security*. Lisbon: Springer, pp. 16-29.
- Bishop, M. & Elliott, C., 2011. *Robust Programming by Example*. Lucerne, Switzerland, Proceedings of 7th Word Conference on Information Security Education.
- Bloom, B. (. E. M. F. E. H. W. K. D., 1956. *Taxonomy of Educational Objectives, Handbook I.*. Allyn & Bacon ed. New York: Pearson.
- Bloomberg Business, 2011. *The Problem with Password*. [Online]
Available at:
http://www.bloomberg.com/bw/magazine/content/11_06/b4214036460585.htm
[Accessed 25 March 2013].
- Boonkrong, S., 2017. Internet Banking Login with Multi-Factor Authentication. *KSI Transactions on Internet and Information Systems*, 11(1), pp. 511-535.
- Brown, N. C. C. et al., 2013. *Bringing Computer Ccience Cack Into Schools: Lessons From The UK*. Denver, Proceedings of the 44th ACM Technical Symposium On Computer Science Education, pp. 269-274.
- BROWN, N. C. C., SENTANCE, S., CRICK, T. & HUMPHREYS, S., 2014. Restart: The Resurgence of Computer Science in UK Schools. *ACM Transactions on Computing Education (TOCE)*, 14(2), p. 9.
- Burton, C., 2005. Replicating the Manchester Baby: motives, methods, and messages from the past. *IEEE Annals of the History of Computing*, July-Sept, Volume 27-3, pp. 44-60.
- Caixa Econômica Federal, n.d. *Caixa*. [Online]
Available at: www.caixa.gov.br
[Accessed 20 10 2020].
- Carrier, B., 2002. *Open Source Digital Forensics Tools: The Legal Argument*. [Online]
Available at:
http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf
[Accessed 25 November 2014].
- CARRIER, B., 2002. Open Source Digital Forensics Tools: The Legal Argument. *Packetstormsecurity*, 10 10.
- CARRIER, B., 2005. *File System Forensic Analysis*. New Jersey: Addison-Wesley.

Casey, E. & Stellatos, G. J., 2008. The Impact of Full Disk Encryption on Digital Forensics. *ACM SIGOPS - Operating Systems Review (OSR)*, Vol 42(Issue 3), pp. 93-98.

Cebula, J. J. & R.Young, L., 2010. *A Taxonomy of Operational Cyber Security Risks*, Hanscom: Software Engineering Institute of Carnegie Mellon.

Cecília Regina Oliveira Assis et al., 2019. *A Comparative Analysis of Classifiers in the Recognition of Packed Executables*. s.l., s.n.

Chandler, S., 2020. *Forbes.com*. [Online]
Available at: <https://www.forbes.com/sites/simonchandler/2020/06/08/nasa-hit-by-366-rise-in-cybersecurity-incidents-after-budget-cuts/?sh=5827e6105b31>
[Accessed 08 09 2021].

Check Point Software Technologies Ltd, 2014. *Check Point Security Report 2014*. [Online]
Available at: <https://www.checkpoint.com/documents/ebooks/security-report-2014/files/assets/common/downloads/Check%20Point%20Security%20Report%202014.pdf>
[Accessed 19 07 2020].

Chivers, H., 2014. Private browsing: A window of forensic opportunity. *Digital Investigation*, 11(1), p. 20–29.

Chris Baraniuk, BBC News, 2015. *Ashley Madison: 'Suicides' over website hack*. [Online]
Available at: <https://www.bbc.com/news/technology-34044506>
[Accessed 20 05 2020].

Christey, S., 2011. *CWE/SANS Top 25 Most Dangerous Software Errors*. [Online]
Available at: <http://cwe.mitre.org/top25/>
[Accessed 20 December 2014].

Chrysikos, A., Ahmed, E. & Ward, R., 2017. Analysis of Tinto's student integration theory in first-year undergraduate computing students of a UK higher education institution. *International Journal of Comparative Education and Development*, 19 10, pp. 97-121.

CISCO, 2008. *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. [Online]
Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html
[Accessed 24 February 2014].

CISCO, 2014. *DataLeakageWorldwide:CommonRisksandMistakes Employees Make..* [Online]
Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html

Coffey, J. W., n.d. An Analysis of Inadvertent Data Disclosure Incidents, 2005-2017. *IJCSDf*, Volume Vol 6 -2, pp. 84-91.

COMPUTERWORLD, 2007. *Pesquisa: Gestores de TI admitem vasculhar e-mails privados de funcionários*. [Online]
Available at: <http://computerworld.com.br/seguranca/2007/05/29/idnoticia.2007-05-29.8374230723/>
[Accessed 21 February 2014].

Consumer Watch, 2015. *Testing firm picks Kaspersky and Bitdefender as the best antivirus suites of 2015*. [Online]
Available at: <http://web-ebshost.ez106.periodicos.capes.gov.br/ehost/pdfviewer/pdfviewer?vid=0&sid=921>

b44a4-4174-45ae-8223-4562b8458cf5%40sdc-v-sessmgr02
 [Accessed 20 07 2020].

Courrejou, T. & L. Garfinkel, S., 2011. *A COMPARATIVE ANALYSIS OF FILE CARVING SOFTWARE*. [Online]
 Available at: <http://www.dtic.mil/dtic/tr/fulltext/u2/a550119.pdf>
 [Accessed 20 November 2014].

Cox, A. M., 2006. *Portals: people, processes and technology*. s.l.:Facet Publishing.

Crane, C., 2020. *The Definitive Cyber Security Statistics Guide for 2020*. [Online]
 Available at: <https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/>
 [Accessed 17 07 2020].

CSO, 2020. *Top cybersecurity facts, figures and statistics for 2020*. [Online]
 Available at: <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>
 [Accessed 17 07 2020].

Cybermetrics, 2018. *Webometrics*. [Online]
 Available at: <http://www.webometrics.info>
 [Accessed 04 02 2018].

Dawson, M., 2017. *Hyper-connectivity: Intricacies of national and international. Doctoral Thesis at London Metropolitan*.

De Gruyter, 2018. *Journal of Homeland Security and Emergency Management*. [Online]
 Available at: <https://www.degruyter.com/view/j/jhsem?lang=en>
 [Accessed 23 03 2020].

Delamaro, M. E., Maldonado, J. C. & Jino, M., 2007. *Introdução ao Teste de Software*. 1 ed. Rio de Janeiro: Elsevier.

DELAMARO, M. E., MALDONADO, J. C. & JINO, M., 2007. *Introdução ao Teste de Software*. 1 ed. Rio de Janeiro: Elsevier.

Department for Digital, C. M. a. S., 2019. *Cyber Security Breaches Survey 2019*, London: UK Government.

Department Homeland Security, 2009. *A Roadmap for Cybersecurity Research*. [Online]
 Available at: <http://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>
 [Accessed 10 February 2016].

Die.net, 2009. *strings(1) - Linux man page*. [Online]
 Available at: <http://linux.die.net/man/1/strings>.
 [Accessed 30 June 2012].

Dienlin, T. & Trepte, S., 2014. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 31 July.

Discovery Channel, 2012. *Discovery website*. [Online]
 Available at: <http://dsc.discovery.com>
 [Accessed 07 October 2012].

DW, 2015. *Poland's pre-war code crackers*. [Online]
 Available at: <https://www.dw.com/en/polands-pre-war-code-crackers/a-18267853>
 [Accessed 24 10 2020].

EICAR, 1998. *Anti-malware Test File*. [Online]
 Available at: <http://www.eicar.org/>
 [Accessed 23 January 2016].

Ellacott, J., 2014. *Leading Email Encryption Vendors Respond to Heartbleed Bug Threat*. [Online]
Available at: <http://www.technavio.com/report/global-email-encryption-market-2014-2018>
[Accessed 22 February 2015].

Escola Superior de Guerra, 2013. CAMPOS DE ATUAÇÃO DO PODER NACIONAL . In: *Manual Básico da Escola Superior de Guerra - Elementos Fundamentais Volume I*. Rio de Janeiro: Biblioteca General Cordeiro de Farias, pp. 66 - 84.

Escola Superior de Guerra, 2014. *BRASIL : ESCOLA SUPERIOR DE GUERRA. Manual Básico, vol I, Elementos Fundamentais.*, Rio de Janeiro: s.n.

EUROPEAN EXPERT GROUP FOR IT-SECURITY, 2020. *EICAR*. [Online]
Available at: www.eicar.org
[Accessed 19 07 2020].

European, C., 2017. *Cybersecurity Act, COM(2017) 477 final, 13.9.201*, Brussels: European Commission.

Farid Daryabar, e. a., 2011. Investigation of Malware Defense and Detection Techniques. *IJCSDF International Journal of Cyber Security and Digital Forensics* 1(3) , pp. 645-650.

Ferrari, A., 2013. *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*, Seville : European Commission Institute for Prospective Technological Studies.

Filatov, A., 2015. *Data Security Solution*. [Online]
Available at: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress2014-arrowecs-roadshow-baltics>

Filatovs, A., 2014. *Data Security Solutions*. [Online]
Available at: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress-2014-arrowecs-roadshow-baltics>.
[Accessed 25 February 2015].

Filiol, E., 2005. *Computer viruses: from theory to applications*. France: Springer Verlag .

FLEISHMAN, G., 2018. BITDEFENDER ANTIVIRUS FOR MAC: A PERFORMANCE JUMP MAKES IT FAR MORE RELIABLE. *MacWorld*, Volume August, pp. 93-97.

Ford, R., 2004. The future of virus detection. *Information Security Technical Report* Vol. 9, No. 2, pp. 19 - 26.

Foremost, n.d. *Foremost*. [Online]
Available at: <http://foremost.sourceforge.net>
[Accessed 15 08 2013].

Foundation, T., 2013. *Truecrypt*. [Online]
Available at: <http://truecrypt.org>

FU, K. S. K. F. N., 2001. *Dos and Don'ts of Client Authentication on the Web*. Whashington DC, s.n.

FU, K. S. K. F. N., 2001. *Dos and Don'ts of Client Authentication on the Web*. Whashington DC, s.n.

G1, 2013. *Petrobras afirma que informações sigilosas foram furtadas*. [Online]
Available at: http://g1.globo.com/Noticias/Economia_Negocios/0,,MUL298824-9356,00INFORMACOES+SIGILOSAS+SAO+FURTADAS+D+A+PETROBRAS.html

Gabet, R. M., 2016. *A comparative forensic analysis of privacy enhanced web*

browsers". s.l.:s.n.

Gal-Ezer, J., Beerli, C., Harel, D. & Yehudai, A., 1995. A High-School Program in Computer Science. *Computer*, 28(10), pp. 73-80.

GALLIANO, A. G., 1979. O método científico: teoria e prática. In: São Paulo: Editora Mosaico, p. 6.

Ghemri, F. & Bouras, A., 2018. *Innovative Education in Cyber Security Field through Collaborative Education Academic/Industry*. Bangkok, The 2018 Technology Innovation Management and Engineering Science International Conference (TIMES-iCON2018), pp. 1-15.

Ghostcrypt, 2018. *Ghostcrypt*. [Online]

Available at: <https://www.gostcrypt.org/>

Ghostcrypt, 2018. *Ghostcrypt*. [Online]

Available at: <https://www.ghostcrypt.org/>

Gibbs, S., 2014. *The Guardian*. [Online]

Available at: <https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec>

[Accessed 06 05 2014].

Google Inc., 2014. *Chrome*. [Online]

Available at: <https://www.google.com.br/chrome/browser/desktop/index.html>

[Accessed 15 November 2014].

Google, n.d. *Integrating Google Sign-In into your web app*. [Online]

Available at: <https://developers.google.com/identity/sign-in/web/sign-in>

[Accessed 24 10 2020].

Gould, D. A., Block, G. & Cleveland, S., 2020. Evolutionary and Ideation Concepts for Cybersecurity Education. *International Journal of Smart Education and Urban Society*, 11(1), pp. 13-22.

Greenberg, A., 2010. *Symantec Acquires Encryption Provider PGP For \$300 Million*. [Online]

Available at: <http://www.forbes.com/sites/firewall/2010/04/29/symantec-acquires-encryption-provider-pgp-for-300-million/>

[Accessed 24 February 2015].

Grispos, G., Storer, T. & Glisson, W. B., 2011. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digital Investigation*, 20 July, pp. 23-26.

Hachman, M., n.d. *The Best Windows 8.1 Antivirus Software*. [Online]

Available at: <http://web-a->

[ebSCOhost.ez106.periodicos.capes.gov.br/ehost/pdfviewer/pdfviewer?vid=1&sid=71fc32f5-c75d-48b3-aff1-8bc45bf482be%40sdc-v-sessmgr01](http://web-a-ebSCOhost.ez106.periodicos.capes.gov.br/ehost/pdfviewer/pdfviewer?vid=1&sid=71fc32f5-c75d-48b3-aff1-8bc45bf482be%40sdc-v-sessmgr01)

[Accessed 20 07 2020].

HANSMAN, S. H. R., 2004. A Taxonomy of Network and Computer Attacks. *Computers & Security*.

Hanushek, E. A. & Woessmann, L., 2020. *The Economic Impacts of Learning Losses*, s.l.: OECD.

HESA, 2018. *Higher Education Statistics Agency: UK, 2016/17*, Promenade: HESA.

Hesham Alshaikh, e. a., 2020. Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, Volume 117(40), pp. 31-39.

History Channel, 2014. *History.com website*. [Online]

Available at: <http://www.history.com>

[Accessed 10 September 2014].

HOWARD, J. D., 1997. *An analysis of Security Incidents on the Internet 1989-1995*.

PhD Thesis., s.l.: Carnegie Mellon University.

HOWARD, M. L. D. V. J., 2010. *24 Deadly Sins of Software Security - Programming Flaws and How to Fix Them*. New York: McGrawHill:.

ICSA Labs, 2014. *ISCA LABS. ICSA Labs Anti-Virus Certification Test Matrix*. [Online]
Available at: <https://www.icsalabs.com/technology-program/anti-virus/av-monthly-testing-reports>
[Accessed 19 07 2020].

IDRIX, 2018. *Veracrypt*. [Online]
Available at: <https://veracrypt.codeplex.com/>

IDRIX, 2018. *VeraCrypt*. [Online]
Available at: <https://veracrypt.codeplex.com/>

IFSP, 2017. *Federal Institut of Education of São Paulo*. [Online]
Available at: www.ifsp.edu.br

IT Services, The University of Manchester,, 2014. *Encryption software*. [Online]
Available at:
<http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/>

Jing-Chiou Liou*, M. L. T. W. L. D. P. S. S., 2016. *A Study of the Internet Privacy in Private Browsing Mode*. s.l., s.n.

Joshi, A. et al., 2012. *Student Centric Design for Cyber Security Knowledge Empowerment*. Kerala, , IEEE International Conference on Technology Enhanced Education (ICTEE), pp. 1-4.

Kakizaki, Y., 2016. Online Accounts Management Method Using Risk-Based Approach. *Journal of Computer and Communications*, Volume 4, pp. 26-36.

Kessler, G. C. & Ramsay, J. D., n.d. *A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students*. s.l., 2014 47th Hawaii International Conference on System Science.

KHU-SMITH, V. M. C., 2002. Enhancing the Security of Cookies. *Lecture Notes in Computer Science*, V(2288), pp. 132-145.

Kimak, S., 2016. *An Investigation into Possible Attacks on HTML5 IndexedDB and their Prevention..* s.l.:s.n.

KNUDSEN, L. R., 1999. Block Ciphers — A Survey. In: *State of the Art in Applied Cryptography*. Belgium: Springer Berlin Heidelberg, pp. 18 - 48.

Kornblum, J., Kendall , . K. & Mikus, N., 2002. *Foremost website*. [Online]
Available at: <http://foremost.sourceforge.net/>
[Accessed 12 October 2012].

Kovacs, E., 2021. *Securityweek*. [Online]
Available at: <https://www.securityweek.com/nasa-identified-over-6000-cyber-incidents-past-4-years>
[Accessed 08 09 2021].

Kuraku, S. & Kalla, D., 2020. Emotet Malware -A Banking Credentials Stealer. *IOSR Journal of Computer Engineering*, 22(4), pp. 31-40.

Langner, R., 2013. *To Kill a Centrifuge*, Arlington | Hamburg | Munich: The Langner Group.

Lasiello, E., 2015. Are Cyber Weapons Effective Military Tools?. *Military and Strategic Affairs*, pp. 23-40.

Lee , S., Savoldi, A., Lee, S. & Lim, J., 2007. *Windows Pagefile Collection and Analysis for a Live Forensics Context*. Jeju-Island, Korea, s.n.

Lewis, M. N. & Nguyen, T. H., 2020. Unifying People, Process, and Technology. In: *Transforming Healthcare Analytics*. s.l.:s.n.

- Lodgher, A., Yang, J. & Bulut, U., 2008. *An Innovative Modular Approach of Teaching Cyber Security across Computing Curricula*. San Jose, CA, IEEE Frontiers in Education Conference (FIE), pp. 1-5.
- LOUGH, D. L., 2001. *A Taxonomy of Computer Attacks with Applications to Wireless Networks*. PhD Thesis., s.l.: Virginia Polytechnic Institute and State University.
- Ludwig, M., 1995. *The Giant Black Book of Computer Viruses*. Show Low, Arizona: American Eagle Publications, Inc..
- Ludwig, M. A., 1993. *Computer Viruses, Artificial Life and Evolution*. Tucson, Arizona: American Eagle Publications, Inc..
- Maclean, W., 2011. Analysis: Cyber raids fuel calls for training, monitoring. *Reuters*, 17 06.
- Mahendrakar, A., Irving, J. & Patel, S., 2010. *Forensic Analysis of Private Browsing Mode in Popular Browsers*. [Online]
Available at: <http://mocktest.net/paper.pdf>
[Accessed 30 November 2014].
- Martti Lehto, 2020. *Cyber security capacity building – cyber security education in Finnish universities*. Jyväskylä, University of Jyväskylä.
- McAfee Company, 2013. *Infografic The State of Malware*. [Online]
Available at: <http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx>
[Accessed 10 February 2014].
- McAfee, J., n.d. *John McAfee: The death of antivirus*. [Online]
Available at: <https://www.ibtimes.co.uk/john-mcafee-death-antivirus-1507388>
[Accessed 20 07 2015].
- Md Saidi Raihana et al., 2017. *Analysis of Private Browsing Activities*. s.l., s.n., pp. 217-228.
- Microsoft Corp., n.d. *Ten Immutable Laws Of Security*. [Online]
Available at: <https://technet.microsoft.com/en-us/library/hh278941.aspx>
[Accessed 22 February 2014].
- Microsoft, 2014. *What is InPrivate Browsing?*. [Online]
Available at: <http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing#1TC=windows-7>
[Accessed 15 November 2014].
- Miller, G., 2016. *60% of small companies that suffer a cyber attack are out of business within six months*. [Online]
Available at: <http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>
[Accessed 10 november 2017].
- MJC Huang, S. W., 2018. Security and Tor Forensics. *Communications of the CCISA*.
- Modesti, P., 2020. Integrating Formal Methods for Security in Software Security Education. *Informatics in Education*, 16 09, 19(3), p. 425–454.
- Mohsen Damshenas, e. a., 2013. *IJCSDF - International Journal of Cyber-Security and Digital Forensics* 2(4):10-29, pp. 10-29.
- Montes, A. et al., 2014. *Aplicação do método Brasil de avaliação de anti-malware e as repercussões para a defesa cibernética*. São José Dos Campos, s.n., pp. 177-182.
- Moreira, D., 2009. *Roubo de notebook custa mais de US\$ 115 mil*. [Online]
Available at: <http://info.abril.com.br/noticias/ti/roubo-de-notebook-custa-mais-de-us-115-mil-23042009-11.shl>

[Accessed 21 February 2014].

Morris et al., N., 2018. Investigating Google Chrome 66.0.3359 Artefact: Internet Forensics Approach. *International Journal of Computer Science and Mobile Computing*, Volume 7(7), pp. 112-122.

Mozilla Contributors, 2014. *Private Browsing*. [Online]
Available at: <https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info>
[Accessed 15 November 2014].

Nance, K., Hay, B. & Bishop, M., 2012. *Secure Coding Education: Are We Making Progress?*. Orlando-FL, s.n.

National Aerospace Administration, 2021. *WMAP's Universe*. [Online]
Available at: shorturl.at/eBP29
[Accessed 16 07 2021].

National Science Foundation, 2011. *When viruses infect bacteria: Looking in vivo at virus-bacterium associations*. [Online]
Available at: www.sciencedaily.com/releases/2011/07/110701101748.htm
[Accessed 10 February 2016].

NATO, n.d. *The history of cyber attacks - a timeline*. [Online]
Available at: <https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm>
[Accessed 05 08 2021].

Nelson, J. & Jeske, D., 2013. *Systems and methods for strengthening web credentials*. United States, Patent No. US8381272B1.

Nikolaos Tsalis Et al., 2017. Exploring the protection of private browsing in desktop browsers. *Elsevier Cose*, Volume 67, pp. 81- 197.

Nissim, N., Moskovitch, R., Rokach, L. & Elovici, Y., 2014. Novel active learning methods for enhanced PC malware detection. *Expert Systems with Applications*, pp. 5843-5857.

NSA, 2014. *2014 Hall of Honor Inductee*. [Online]
Available at: <https://www.nsa.gov/About-Us/Current-Leadership/Article-View/Article/1621548/marian-rejewski/>
[Accessed 24 10 2014].

NSS Labs, 2018. *NSS LABS. Endpoint Protection – Evasion and Exploit: Test Methodology*. [Online]
Available at: <https://www.nsslabs.com/reports/evasions-test-methodology-v1-1/>
[Accessed 19 07 2020].

Nurhayati, A., Gautama, A. & Naseer, M., 2018. *Decision making model design for antivirus software selection using Factor Analysis and Analytical Hierarchy Process*. s.l., s.n., pp. 1-6.

Office for National Statistics UK, 2016. *SIC Codes*. [Online]
Available at: <http://www.siccodesupport.co.uk/home/>

Ohana, D. J. & Shashidhar, N., 2013. *Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions*. [Online]
Available at: <http://jis.eurasipjournals.com/content/2013/1/6>
[Accessed 03 December 2014].

Oh, J., Lee, S. & Lee, S., 2011. *Advanced evidence collection and analysis of web browser activity*. New Orleans - USA, s.n., pp. 62-70.

OH, J. L. S. L. S., 2011. Advanced Evidence Collection and Analysis of Web Browser Activity. *Digital Investigation*, 8, pp. 62-70.

OH, J. L. S. L. S., 2011. Advanced Evidence Collection and Analysis of Web

Browser Activity. *Digital Investigation*, 8, pp. 62-70.

Olagbemiro, M. A. O., 2014. *CYBERSPACE AS A COMPLEX ADAPTIVE SYSTEM AND THE POLICY AND OPERATIONAL IMPLICATIONS FOR CYBER WARFARE*. s.l.:USA Air Force.

Oracle, 2013. *VirtualBox*. [Online]
Available at: <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>
[Accessed 13 06 2013].

Oracle, 2014. *Oracle, VM VirtualBox*. [Online]
Available at: <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>
[Accessed 15 November 2014].

Park, K., Ruiz, R. & Montes, A., 2011. *BinStat - Ferramenta para Reconhecimento de Executáveis Empacotados*. Florianopolis, s.n., pp. 173-181.

Park, K., Ruiz, R. & Montes, A., 2012. BinStat Tool for Recognition of Packed Executables. *The International Journal Of Forensic Computer Science - Ijofcs*, Volume 1, pp. 44-58.

Parry, W., 2012. *Viral Attacks on Bacteria Reveal a Secret to Evolution*. [Online]
Available at: <http://www.livescience.com/18144-evolution-trait-virus-bacteria.html>
[Accessed 20 December 2014].

Passey, D., 2017. Computer science (CS) in the Compulsory Education Curriculum: Implications for Future research. *Education and Information Technologies*, Volume 22, p. 401.

Ponemon Institut, 2014. *Expondo as Lacunas da Cibersegurança: Brasil*. [Online]
Available at: <http://www.websense.com/assets/reports/report-ponemon-2014-part1-summary-brazil-pt.pdf>
[Accessed 07 07 2014].

Prof. Alencar de Melo Júnior, e. a., 2017. *Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas*. [Online]
Available at: <https://drive.ifsp.edu.br/s/qe7rqe5Dpq9j3Aa#pdfviewer>

Ramirez, R. B., 2017. *Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization*. Cambridge: Master's thesis in technology and policy, Massachusetts Institute of Technology.

Reza, A. & Shareeful Islam, H. J. a. A. A.-N., 2013. Analyzing Human Factors for an Effective Information Security Management System. *International Journal of Secure Software Engineering (IJSSE)*, 18 9, 4(1), pp. 50-74.

Richard III, G. G. & Roussev, V., 2005. *A Frugal, High Performance File Carver*. New Orleans - USA, s.n.

RICHARD III, G. G. R. V., 2005. *A Frugal, High Performance File Carver*. New Orleans, s.n.

Rodrigo de S. Ruiz et al., F. P. A. a. K. J. B. P. D. S., 2012. *Turning Public the private navigation. Tornando Pública a Navegação "In Private"*. Brasília, s.n., pp. 67-75.

Rodrigo de S. Ruiz et al., F. P. A. K. J. B. P. D. S., 2014. *Security Issue on Cloned TrueCrypt Containers and Backup Headers*. Kuala Lumpur, s.n., pp. 11-19.

Rodrigo Ruiz et al., V. G. T. G., 2019. *Um Cara, 6 passaportes (A Person, With 6 Passports)*. Campinas: Clube dos Autores.

Rodrigo Ruiz, R. W., 2017. Lazarus: Data Leakage With Cryptographic Systems. *Cyber Defense Magazine*, Volume 6, pp. 95-98.

Rogério Winter et al., R. R. A. C. B. M., 2018. Brazilian Cybersecurity – The Challenge Among Technology, Processes, People And Environment. *Critical*

Infrastructure Protection Review, Volume Spring, pp. 37-44.

Rogerio Winter et al., R. R. F. d. F. R. M. J., 2020. *Cyber Mission Operations: A Literature Review*. Las Vegas, s.n.

Rosa, F. d. F., Jino, M. & Bonacin, R., 2018. Towards an Ontology of Security Assessment: a core model proposal. In: *Information Technology - New Generations. Advances in Intelligent Systems and Computing*, vol 738.. s.l.:Springer, Cham..

Rosling, L., 2021. *Need To Know Micro Business Statistics UK 2021*. [Online] Available at: <https://www.smeloans.co.uk/blog/micro-business-statistics-uk/#:~:text=The%20main%20difference%20between%20a,money%20on%20its%20balance%20sheet.> [Accessed 08 09 2021].

Ruiz, N., 2020. Is Brazil taking advantage of COVID-19 to promote age and social extermination?. *Science Magazine*, 03.

Ruiz, N. & Ganzert, T., 2020. *Brazil, the pandemic, the specialization of species and the globalized market*. [Online] Available at: <https://science.sciencemag.org/content/367/6484/1289/tab-e-letters> [Accessed 19 03 2020].

Ruiz, N. & Ganzert, T., 2020. REPRINT -Brazil, the pandemic, the specialization of species and the globalized market. *Critical Infrastructure Protection Review*, 19 March.

Ruiz, N. et al., 2021. *Method and Tool for Generating Table of Relevance in Literature Review (MTTR)*. London, s.n.

Ruiz, N., Shukla, P. & Kazemian, H., 2020. Cyber Security Index For Undergraduate Computer Science Courses in the UK. *Journal of Applied Security Research*.

Ruiz, N., Shukla, P. & Kazemian, H., 2020. Privacy in The First Line of the First Code. *Science Magazine*, 17 04.Issue on-line.

Ruiz, N. et al., 2020. Brazil Method of Anti-malware Evaluation and Cyber Defence Impacts. *Journal of Applied Security Research*.

Ruiz, R., 2011. Brasil, Patent No. Register number 03654-6/2000 - RPI2122.

Ruiz, R., 2013. Um Pouco Sobre Segurança. In: *Sistemas Comerciais. Conceitos Modelagem e Projeto*. s.l.:Ciência Moderna.

Ruiz, R., 2014. Trigona Honey-Client Technical Comparison Report. *Researchgate.net*.

Ruiz, R., 2016. Who is afraid of the sea monsters?. *Cyber Warnings E-Magazine*, Volume November, pp. 84-85.

Ruiz, R., 2017. NK is the new Iraq?. *Cyber Defense Magazine*, Volume 6, pp. 109-111.

Ruiz, R., 2017. Symbiosis and Fear, Evolucionary Benefits of Cybersecurity. *United States Cyber Security Magazine*, Volume Spring, pp. 61-62.

Ruiz, R., 2019. *A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity*. London, s.n., pp. 1-8.

Ruiz, R., 2019. *A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity*. London, s.n., pp. 1-8.

Ruiz, R., Amatte, F. & Park, K., 2014. *Opening the " Private Browsing " Data - Acquiring Evidence of Browsing Activities*. Kuala Terengganu, s.n., p. CD1.

Ruiz, R., Amatte, F. P. & Park, K. J. B., 2014. *Security Issue on Cloned TrueCrypt Containers and Backup Headers*. Kuala Lumpur, Malaysia, SDIWC.

Ruiz, R. d. S., Amatte, F. P. & Park, K. J. B., 2014. *Opening the "Private Browsing" Data – Acquiring Evidence of Browsing Activities*. Kuala Terengganu, Malaysia, s.n., pp. 72 - 79.

- Ruiz, R. d. S., Amatte, F. P. & Park, K. J. B., 2012. *Tornando Pública a Navegação "InPrivate"*. Brasília - Brazil, s.n.
- Ruiz, R. d. S., Amatte, F. P. & Park, K. J. B., 2014. *Security Issue on Cloned TrueCrypt Containers and Backup Headers*. Kuala Lumpur - Malaysia, s.n., pp. 11-19.
- Ruiz, R. d. S., Amatte, F. P., Park, K. J. B. D. S. & Winter, R., 2015. Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode. *International Journal of Cyber-Security and DigitalForensics*, 4(3), pp. 404-416.
- Ruiz, R., Park, K., Amatte, F. & Winter, R., 2015. Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 4(3), pp. 404-416.
- Ruiz, R. & Winter, R., 2015. Apoc@lypse: when the anti-malware is sick. *Cyber Defense Magazine - Cyber Warnings*, pp. 26-28.
- Ruiz, R. & Winter, R., 2016. Corrosive Secrecy and Confidence: the Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security. *Cyber Security Review*, 01 03.pp. 66-74.
- Ruiz, R. & Winter, R., 2016. Lazarus: Data Leakage with PGP and Resurrection of the Revoked User. *Journal of Cyber Security and Mobility*, 1 4, 5(2), pp. 1-14.
- Ruiz, R. & Winter, R., 2016. Lazarus: Data Leakage with PGP and Resurrection of the Revoked User. *Journal of Cyber Security Vol 5 2*, 1-14, 20 11.
- Ruiz, R. & Winter, R., 2016. Lazarus: Data Leakage with PGP and Resurrection of the Revoked User. *Journal of Cyber Security and Mobility*, 20 11, 5(2), pp. 1-14.
- Ruiz, R. & Winter, R., 2016. Reprint: Lazarus: Data Leakage with PGP and Resurrection of the Revoked User. *Cyber Security Review*, Volume Autumn , pp. 47-53.
- Ruiz, R. & Winter, r., 2017. Brazilian "Car Wash" Task Force: Cyber Security Lessons. *Cyber Defense Magazine*, Volume 11, pp. 15-16.
- Ruiz, R. & Winter, R., 2017. *Credentials (UN)Management in home banking*. [Online]
Available at: <https://securityaffairs.co/wordpress/64699/>
- Ruiz, R. & Winter, R., 2017. Spying Across Borders in the Age of Email. *2600 Magazine*, Volume 33(4), pp. 18-24.
- Ruiz, R., Winter, R., Park, K. & Amatte, F., 2015. *Apoc@lypse: The end of antivirus*. North Charleston: North Charleston: CreateSpace Independent Publishing Platform.
- Ruiz, R., Winter, R., Park, K. & Amatte, F., 2016. *Apoc@lypse: O fim do antivirus*. North Charleston: CreateSpace Independent Publishing Platform.
- Ruiz, R., Winter, R., Park, K. & Amatte, F., 2017. The leakage of passwords from home banking sites: A threat to global cyber security?. *Journal of Payments Strategy & Systems*, Volume 11(2), pp. 1-13.
- Ruiz, R., Winter, R., Park, K. & Amatte, F., 2017. The leakage of passwords from home banking sites: A threat to global cyber security?. *Journal of Payments Strategy and Systems Volume 11 / Number 2 / Summer 2017*, pp. 174-186.
- Sadok, M. & Bednar, P., 2015. *Understanding Security Practices Deficiencies: A Contextual Analysis*. In S. Furnell, & N. Clarke (Eds.). Plymouth , Centre for Security, Communications and Network Research, Plymouth University, UK, pp. 151-160.
- Sanders, C., 2010. *How I Cracked your Windows Password (Part 1)*. [Online]
Available at: <http://www.windowsecurity.com/articles->

[tutorials/authentication_and_encryption/How-Cracked-Windows-Password-Part1.html](#)

[Accessed 20 February 2014].

Schneider, F. B., 2013. Cybersecurity Education in Universities. *IEEE Security & Privacy*, Issue July/August 2013, pp. 3-4.

SEACORD, R. C. H. A. D., 2005. *A Structured Approach to Classifying Security Vulnerabilities. Technical Note, CM/SEI-2005-TN-003, Survivable Systems*, s.l.: Carnegie Mellon Software Engineering Institute.

Seapei Nozimballi Mogoane, S. K., 2019. *Challenges in Information and Cybersecurity program offering at Higher Education Institutions*. s.l., Kalpa Publications in Computing, p. 202–212.

Sentance, S., Dorling, M., McNicol, A. & Crick, T., 2012. *Grand challenges for the UK: upskilling teachers to teach computer science within the secondary curriculum*. Hamburg, Proceedings of the Seventh Workshop in Primary and Secondary Computing Education.

Sharipova, Z. B. & Khudayarovich, F. Y., 2021. THE RELEVANCE OF CYBER SECURITY EDUCATION IN THE CLASSROOM. *ACADEMICA An International Multidisciplinary Research Journal*, 5, 11(5), pp. 637-645.

Shevchenko, S. M., Skladannyi, P. M. & Martseniuk, M., 2019. ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. *Cybersecurity: Education, Science, Technique*, 4(4).

Shoeb, A. A. M., 2017. *Is Private Browsing in Modern Web Browsers Really Private?*. [Online]

Available at: <https://www.shoeb.info/wp-content/uploads/abu-shoeb-position-paper-on-private-browsing.pdf>

Shoemaker, D., Kohnke, A. & Sigler, K., 2016. *The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)*. Boca Raton: CRC Press.

Shumaila Alam, M. A. W. I., 2016. Forensic Analysis of Edge Browser InPrivate Mode. *International Journal of Computer Science and Information Security (IJCSIS)*, Volume 14(9).

Shumaila Alam, M. A. W. I., 2017. Forensic Analysis of Edge Browser InPrivate Mod. *e-Forensic Magazine*, Volume 3(6).

Silva, P. D. C. G. d., 2012. *Tecnologia em Análise e Desenvolvimento de Sistemas*. [Online]

Available at:

<http://www.ft.unicamp.br/sites/default/files/graduacao/ProjetoPedagogicoTADS2012.pdf>

Smith, B., Loddo, O. G. & Lorini, G., 2020. On Credentials. *Journal of Social Ontology*, 08, 6(1), pp. 47-67.

Smith, D. M., 2003. The Cost of Lost Data. *Graziadio Business Review*, 6(3).

SOOD, A. K. E. R. J., 2006. A Browser Malware Taxonomy. *VirusBulletin*, 06.pp. 8-13.

Statista.com, 2020. *Proportion of businesses that have experienced cyber security breaches in the UK 2019*. [Online]

Available at: <https://www.statista.com/statistics/586709/proportion-of-businesses-that-have-experience-cyber-security-breaches-in-the-uk/>

[Accessed 17 07 2020].

Strate, L., 1999. The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, 63(3), pp. 382-412.

Studies, C. f. S. a. I., 2014. *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*, s.l.: s.n.

Symantec Corporation, 2014. *Symantec Endpoint Encryption – Protect Your Data*. [Online]
Available at: <https://www.youtube.com/watch?v=NtGSX3pYkLQ>
[Accessed 24 February 2015].

Symantec Corporation, 2015. *How Endpoint Encryption Works*. [Online]
Available at: http://www.symantec.com/content/en/us/enterprise/white_papers/how-endpoint-encryption-works_WP_21275920.pdf
[Accessed 24 February 2015].

Symantec, n.d. *Symantec Desktop Encryption User Manual*. [Online]
Available at:
https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_win_usersguide_en.pdf?_gda_=1475850268_90925006947a919661523e2f67f5cea7
[Accessed 5 10 2016].

Symantec, n.d. *Symantec Desktop Encryption User Manual*. [Online]
Available at:
https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_win_usersguide_en.pdf?_gda_=1475850268_90925006947a919661523e2f67f5cea7
[Accessed 5 October 2016].

Tadmor, A. . D., Ottesen, E. A., Leadbetter, J. R. & Phillips, R., 2011. Probing Individual Environmental Bacteria for Viruses by Using Microfluidic Digital PCR. *Science*, pp. 58-61.

Taylor, B. a. B. M. a. H. E. a. N. K., 2013. *Teaching Secure CodingThe Myths and the Realities*. Denver, Proceeding of the 44th ACM Technical Symposium on Computer Science Education.

Taylor, B. & Azadegan, S., 2005. *Threading secure coding principles and risk analysis into the undergraduate computer science and information systems curriculum*. Kennesaw, Conference: Proceedings of the 3rd Annual Conference on Information Security Curriculum Development, InfoSecCD 2006.

Taylor, C. R. S. a. J. W., 2006. *Computer Security Education: Past, Present*. Monterrey, CA, Seventh Workshop on Education in Computer Security (WECS7).

The New York Times, 2005. *Nytimes*. [Online]
Available at: http://www.nytimes.com/2005/05/10/technology/internet-attack-called-broad-and-long-lasting-by-investigators.html?_r=0
[Accessed 05 01 2016].

Thomas, R., 2003. *Attacks on PGP: A User's Perspective*. [Online]
Available at: <https://www.sans.org/reading-room/whitepapers/vpns/attacks-pgp-users-perspective-1092>
[Accessed 2014].

Tim Fitzsimons, NBC News, 2019. *Tennessee teen's suicide highlights dangers of anti-LGBTQ bullying*. [Online]
Available at: <https://www.nbcnews.com/feature/nbc-out/tennessee-teen-s-suicide-highlights-dangers-anti-lgbtq-bullying-n1060976>
[Accessed 20 05 2020].

Tom Crick, J. H. D. A. I. T. P., 2019. *A UK Case Study on Cybersecurity Education and Accreditation*. Cincinnati, s.n.

Tor Project, 2014. *What is the Tor Browser?*. [Online]

Available at: <https://www.torproject.org/projects/torbrowser.html.en>
[Accessed 15 November 2014].

TRUECRYPT FOUNDATION, n.d. *TrueCrypt*. [Online]
Available at: <http://truecrypt.org>
[Accessed 2013 February 2013].

Tsalis, N., 2017. *Exposing security and privacy liabilities in modern browsers*. s.l.:s.n.

Tytus, n.d. *Genialny matematyk, który łamał Enigmę. Jerzy Różycki (1909–1942)*. [Online]
Available at: <https://tytus.edu.pl/2020/04/02/genialny-matematyk-ktory-lamal-enigme-jerzy-rozycki-1909-1942/>
[Accessed 24 10 2020].

UK Department for Digital, Culture, Media & Sport, 2020. *Research and analysis Cyber security skills in the UK labour market 2020*. [Online]
Available at: <https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020>
[Accessed 17 07 2020].

UNICAMP, 2017. *State University of Campinas*. [Online]
Available at: www.unicamp.br

Universities Central Council on Admissions, 2018. *Universities Central Council on Admissions*. [Online]
Available at: <https://www.ucas.com/ucas-terms-explained>
[Accessed 01 February 2018].

University of Exeter, 2014. *Important information for users of TrueCrypt on Windows laptops*. [Online]
Available at: <http://www.exeter.ac.uk/ig/infosec/encryptionforlaptops/usingtruecrypt/>

University of Michigan, 2018. *Safe Computing*. [Online]
Available at: <https://www.safecomputing.umich.edu/be-aware/privacy/resources>

Valdi, A. et al., 2015. Scalable Testing of Mobile Antivirus Applications. *Computer*, 48(11), pp. 60-68.

Vasilij, K. I., 2018. Sociological assessment of personnel as a factor in ensuring corporation information security. *Tomsk State University Journal of Philosophy, Sociology and Political Science*, Volume 44, pp. 169-182.

Vaughan, C., 2004. Xbox Security Issues and Forensic Recovery Methodology (Utilising Linux). *Digit. Investigation*, September, 1(3), pp. 165 -172.

Virus Bulletin, 2014. *Virus Bulletin Testing Methodology*. [Online]
Available at: <https://www.virusbtn.com/vbspam/methodology/index>
[Accessed 10 04 2014].

Vitorino, T. A. S., 2013. *Análise De Malware Em Ambiente Windows*. s.l.:s.n.

VMware, 2014. *All Downloads*. [Online]
Available at: <https://my.vmware.com/web/vmware/downloads>
[Accessed 20 November 2014].

Wake Forest University School of Business, 2018. *MSBA Software Instalation*. [Online]
Available at: business.wfu.edu/msba-software

Wake Forest University, 2014. *TrueCrypt install*. [Online]
Available at: <http://users.wfu.edu/yipcw/is/truecrypt/>

Wang, P., Dawson, M. & Williams, K. L., 2019. Improving Cyber Defense Education Through National Standard Alignment: Case Studies.. In: *National Security: Breakthroughs in Research and Practice*, edited by Information Resources.

- s.l.:Management Association, IGI Global, pp. 78-91.
- Wang, P., Dawson, M. & Williams, K. L., 2019. Improving Cyber Defense Education Through National Standard Alignment: Case Studies.. In: I. R. M. Association, ed. *National Security: Breakthroughs in Research and Practice*. Information Resources Management Association, 78-91 ed. Hershey, PA: IGI Global, pp. 78-91.
- Weinberger, S., 2011. Is this the start of Cyberwarfare?. *Nature*, 474(8 June 2011), pp. 142 - 145.
- Wen, S.-F., 2020. *A Multi-Discipline Approach for Enhancing Developer Learning in Software*. Gjøvik: s.n.
- West Coast Labs, 2014. *WEST COAST LABS. Technology Reports*. [Online]
Available at: <http://www.westcoastlabs.org>
[Accessed 10 02 2014].
- WinHex, n.d. *WinHex*. [Online]
Available at: <http://winhex.com/winhex/>
[Accessed 20 01 2013].
- Winter, R. & Ruiz, R., 2015. *Luke 8:17 - Errors that Compromise the Privacy and Information Security*. Bucharest, s.n.
- Winter, R. & Ruiz, R., 2016. Apoc@lypse: The End Of Antivirus. When The Antivirus Is The Threat. *Cyber Security Review*, Volume Spring, pp. 58-65.
- Winter, R. & Ruiz, R., 2016. Corrosive Secrecy And Confidence: The Paradox Among Bypassing Cryptographic Software. *Cyber Security Review*, Volume Spring, pp. 66-74.
- Winter, R. & Ruiz, R., 2016. Corrosive Secrecy and Confidence: The Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security. *Cyber Security Review*, 01 03.pp. 66-74.
- Winter, R. & Ruiz, R., 2017. Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life. *International Journal of Cyber-Security and Digital Forensics*, Volume 7(1), pp. 21-30.
- Winter, R. & Ruiz, R., 2017. Cybersecurity, Cyber Weapons And Cyber-Attacks: Responsibility And Different Reflections. *Critical Infrastructure Protection Review Magazine*, Volume 2, pp. 77-82.
- World Economic Forum, 2018. *Global Risks Report 2018*, Geneva: World Economic Forum.
- X-Ways Software Technology AG, 2014. *WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor*. [Online]
Available at: <http://www.x-ways.net/winhex/>
[Accessed 10 November 2014].
- Yaokumah, W., 2019. Cyber Security Competency Model Based on Learning Theories and Learning Continuum Hierarchy. In: *Global Cyber Security Labor Shortage and International Business Risk*. s.l.:IGI Global, pp. 94-110.
- Yue, C., 2016. *Teaching Computer Science With Cybersecurity Education Built-in*. Austin, 2016 USENIX - Workshop on Advances in Security Education.
- Zatko, S., 2016. Rethinking the Role of Security in Undergraduate Education. *IEEE Security & Privacy*, Issue March/April 2016, pp. 73-78.
- Zhao, Z.-S.et al., 1998. Molecular Mimicry by Herpes Simplex Virus–Type 1: Autoimmune Disease After Viral Infection. *Science Vol. 279*, pp. 1344-1347.
- Zoto, E., Kowalski, S., Lopez-Rojas, E. A. & Kianpour, M., 2018. *Using a socio-technical systems approach to design and support systems thinking in cyber security education*. s.l., Proceedings of STPIS'18.

Appendix A Metrics

The total of publications in the specific area of Cyber Security that none appears in other Ph.D. thesis areas is 16. This number affirms the time dedication for Cyber Security studies. It is possible to verify the concentration in the correlated areas like Privacy, Protection Systems, Military operations, and Software.

The Main Contribution reveals the kind specific research the suite of work provides for Computer Science and pears. The number very important to guide the author and supervisors during the analysis of the work. Delivering methods to bypass security systems the author contributes to customers, researchers, vendors, and governments to improving more security and conscience, to preserve privacy, financial resources and lives.

This compendium of the published work submitted for an award is distributed in four kinds of publications: magazines, International Academic Conferences, contributions in academic journals, and a book.

Below it is possible to see the 22 exclude self-citations in languages like English, Japanese, Russian and Portuguese, including the title, authors, local, and the text of citation when it is available.

Citations of (Ruiz, 2019)

1. A UK Case Study on Cyber Security Education and Accreditation (Tom Crick, 2019)
 - *“The UK situation is distinctly different: 61% of UK courses offer mandatory Cyber Security content, and this research was based on web scraping [35, Table 1]. As such it represents a lower bound since not all coverage will necessarily be clearly articulated in publicly available documentation online. It is at least plausible to attribute this difference to differences in the accreditation regimes, as the external circumstances, governmental pressures, and professional body/learned society curricula are all similar.”*

2. Challenges in Information and Cyber Security program offering at Higher Education Institutions (Seapei Nozimballi Mogoane, 2019)
 - *“These findings reaffirm Ruiz’s (2019) position that Cyber Security courses need to be transformed towards a multidisciplinary direction that involves...”*
3. A Multi-Discipline Approach for Enhancing Developer Learning in Software Security (Wen, 2020)
 - *“Many computer science courses such as programming and system development leave software security out of their mandatory curricula”*

Citations of (Ruiz, et al., 2017)

1. Cyber Security Competency Model Based on Learning Theories and Learning Continuum Hierarchy (Yaokumah, 2019)
2. Козачок В. И. Социологическая оценка персонала как фактор обеспечения информационной безопасности корпорации // Вестн. Том. гос. ун-та. Философия. Социология. Политология. Sociological Assessment Of Personnel As A Factor For Security Of Corporation). (Vasiliy, 2018)
 - *“For all recorded incidents, a common trend is revealed during the investigation: almost 37% of violations occurred through the fault of employees, but not intentionally (consciously), but because of inattention or as a result of errors [5–8] “*

Citations of (Park, et al., 2012)

1. A Comparative Analysis of Classifiers in the Recognition of Packed Executables (Cecília Regina Oliveira Assis et al., 2019)
 - *“Based on the methodology proposed by [3], the BinStat tool [4], [5] aims to detect packed executables by extracting information about such files and then applying data mining methods”*

Citations of (Park, et al., 2011)

1. (Malware analysis in Windows) Análise De Malware Em Ambiente Windows (Vitorino, 2013)
 - *“The number of different targets combined with the different objectives of the attacks committed by malicious software in conjunction with the vast arsenal of tools available to developers generates an amount of malware that requires the maximum amount of automation of analysis and prospecting tasks. One of the problems to be treated for static analysis is packaging. In this context, Park et al. (2011) present a methodology for the recognition of executable packaging, by means of the use of statistical calculations and information theory. “*
2. A Comparative Analysis of Classifiers in the Recognition of Packed Executables (Cecília Regina Oliveira Assis et al., 2019)

- *“Based on the methodology proposed by [3], the BinStat tool [4], [5] aims to detect packed executables by extracting information about such files and then applying data mining methods”*

Citations of (Winter & Ruiz, 2017)

1. Ransomware Prevention and Mitigation Techniques (Hesham Alshaikh, 2020)
 - *“Different perspectives adopted by, Winter et al. [19] they emphasize that technology is not improving as fast as the complexity of threats. They have started a cyber-autoimmune disease where an antivirus system is responsible for destroying the computer's operating system after they infected system files with malicious code. To draw interest to flaws in protection systems which, allow attackers to reach their targets more easily causing serious damage.”*
 - *“Contribution: Started a cyber-autoimmune disease; Pros: Emphasize that technology is not evolving as fast as the complexity of threats; Cons: There is no specific solution proposed other than requesting anti-virus companies to update their inefficient methods and techniques.”*

Citations of (Ruiz, et al., 2014)

1. Security and Tor Forensics (MJC Huang, 2018)
2. A Study of the Internet Privacy in Private Browsing Mode (Jing-Chiou Liou*, 2016)

Citations of (Ruiz, et al., 2015)

1. Is Private Browsing in Modern Web Browsers Really Private (Shoeb, 2017)
2. Exploring the protection of private browsing in desktop browsers (Nikolaos Tsalis Et al., 2017)
 - *“Ruiz et al., (2015) focused on recovery techniques for page related data (i.e., text and graphics) created during private browsing. The authors performed their tests within 4 individual phases: shutdown, freeze, kill process and power down, while each phase indicated the way the browser was terminated (e.g., kill process - browser interruption). Their results showed that all phases included flaws regarding user's privacy, in terms of acquiring browsing artefacts. In addition, Montasari and Peltola, (2015) analysed both system's locations and RAM, in all browsers except Opera. Although the selected operating system is not clarified, it is implied that the authors used Windows for their experiments. Their results showed that Chrome is the most secure browser, since there are no artefacts available after private browsing, while Firefox only included low risk artefacts.”*
3. An Analysis of Inadvertent Data Disclosure Incidents (Coffey, s.d.)
 - *“Ruiz et al [7] state that inadvertent data disclosures can sometimes occur when end-users have some expectation of privacy, as in browsing in a private browsing mode. They enumerate four different potential gatherers of information in the browsing chain that could compromise privacy and cause unintended disclosures.*

One might consider this situation to be another example of human error, although this time the error lies in trusting software rather than in outright dangerous behaviours or negligence.”

4. Forensic Analysis of Edge Browser InPrivate Mode (Shumaila Alam, 2016)
 - *“However, few researchers [2], [9], [10] practically proved that mostly web browsers were not efficient to maintain sufficient protection, even with the implementation of private browsing mode.”*
5. Online Accounts Management Method Using Risk-Based Approach (Kakizaki, 2016)
 - *“Ruiz et al . [17] researched personal behaviours regarding privacy that allows the leakage of information.”*
6. Exposing security and privacy liabilities in modern browsers (Tsalis, 2017)
 - *“Ruiz et al., (2015) focused on recovery techniques for page related data (i.e.,text and graphics) created during private browsing. The authors performed their tests within 4 individual phases: shutdown, freeze, kill process and power down, while each phase indicated the way the browser was terminated (e.g.,kill process –browser interruption). Their results showed that all phases included flaws regarding user’s privacy, in terms of acquiring browsing artefacts.”*
7. An Investigation into Possible Attacks on HTML5 (Kimak, 2016)
 - *“Data privacy and information leakage is, therefore, a serious concern(Ruiz et al. 2015).”*
8. A comparative forensic analysis of privacy enhanced web browsers (Gabet, 2016)
 - *“In their 2015 paper, researchers Ruiz, Amatte, Park, and Winter (2015)explored a method to capture data that had been created in a private browser.Contrary to much of the previously reviewed literature, this research did not seek to identify issues with private browsing modes or test the anonymity of private browsers. Instead this research identified a process for collecting artifacts that would disprove the alleged privacy of browser vendors (Ruiz et al., 2015). If successful, the process would have served as a method for assessment and validation of private browser techniques (Ruiz et al., 2015). The methodology that Amatte et al. used tested the browsers Internet Explorer 10, Firefox version 24, Google Chrome version 30, and Safari version 5 on a virtual machine using a four part test. The test SFKP is an acronym for the following; S for shutdown, F for freeze, K for kill process and P for power down. Each of these tests involved generating specific browser data then capturing an image of the virtual machine at a different state to see what happened to the artifacts and if they could be recovered. The results of this study showed that during different machine states, different artifacts were recoverable from each browser. The researchers concluded from this study that the privacy that is being guaranteed in private browsers by browser vendors is not actually being delivered, presenting a much larger problem in a society where web privacy is becoming a large demand (Ruiz et al., 2015)”*
 - *“What this study found was that not only did all of the browsers analysed by the author produce recoverable artifacts, based on research completed by others, every other browser analysed produces recoverable artifacts as well. While this scenario is favorable for*

investigators or law enforcement seeking to use this information for investigative purposes, as Ruiz et al. (2015) states, claims of complete privacy by web browser vendors is still not being delivered”

9. Forensic Analysis of Edge Browser *InPrivate* (Shumaila Alam, 2017)
 - *“However, few researchers [2], [9], [10] practically proved that mostly web browsers were not efficient to maintain sufficient protection, even with the implementation of private browsing mode.”*
10. Investigating Google Chrome 66.0.3359 Artefact: Internet Forensics Approach (Morris et al., 2018)
 - *“This study is similar to the one carried out by [15, 16, 17, 18, 19, 20, 21, 22] which investigated how artefacts are mined in private browsers. The researchers however did not address artefacts left on lifeless imaging. The researcher did also not address the use of extensions to clear browsing data on chrome and their implications to chrome forensic artefacts investigation”*
11. Analysis of Private Browsing Activities (Md Saidi Raihana et al., 2017)
 - *“Forensic examinations of private and portable web browsing artifacts are extremely valuable only if prior research gain de lack significant findings or does not provide suficient answers (Oh and Lee 2011; Ruiz et al. 2015)”*

Researchgate and Google Scholar

Specifically to the School of Computing of London Metropolitan University, I contribute with my index in Researchgate as seen in Figure 23. I figure in march/2020 in the top 10 of a popular member for reading my articles. I also contributed by taking the name of the University in on-line publications at Science Magazine. (Ruiz, et al., 2020) (Ruiz & Ganzert, 2020). In Figure 24 is possible to see the Researchgate Score. Even with some questions, the Researchgate score serves as a good indicator of the reach and relevance in transmitting the knowledge developed in the researcher's articles. Even the Google Scholar H Index Figure 25 is also subject to criticism. The number of citations does not necessarily indicate the impact of research on society and the researcher's ability to pay for open access to articles, and whether the researcher acts as a teacher can create wide disparities.

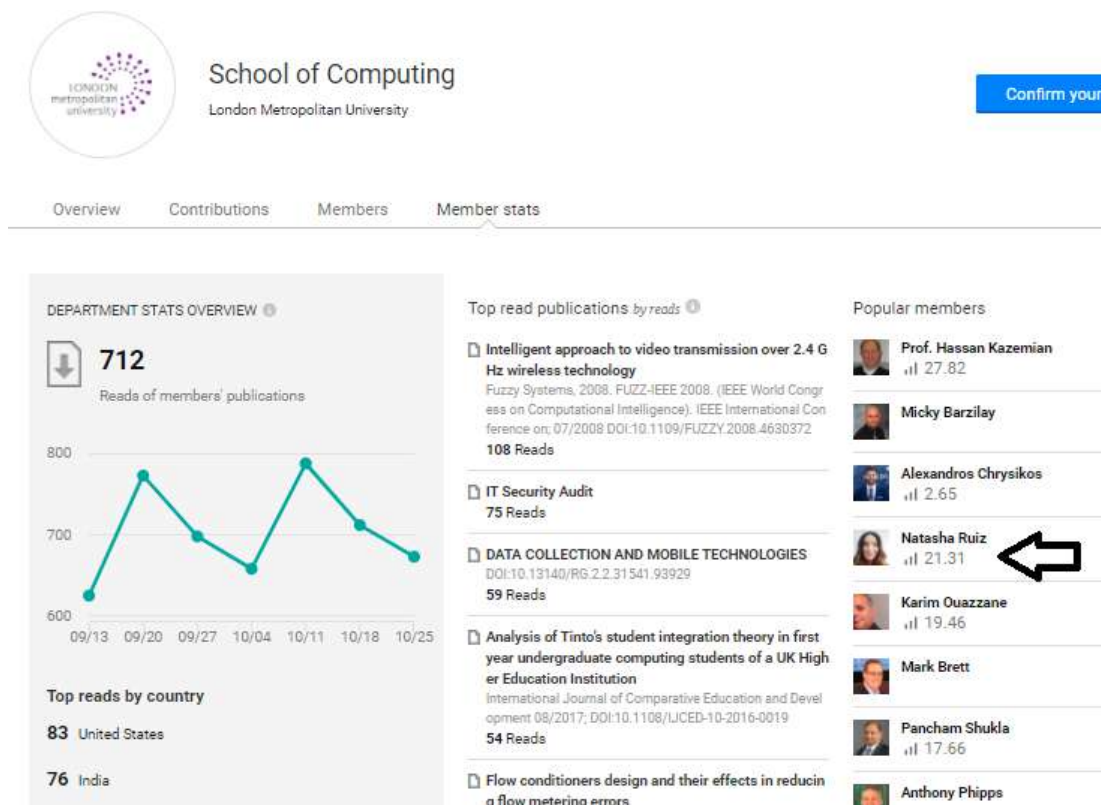


Figure 23 - Researchgate statistics of the School of Computing of London Metropolitan University.

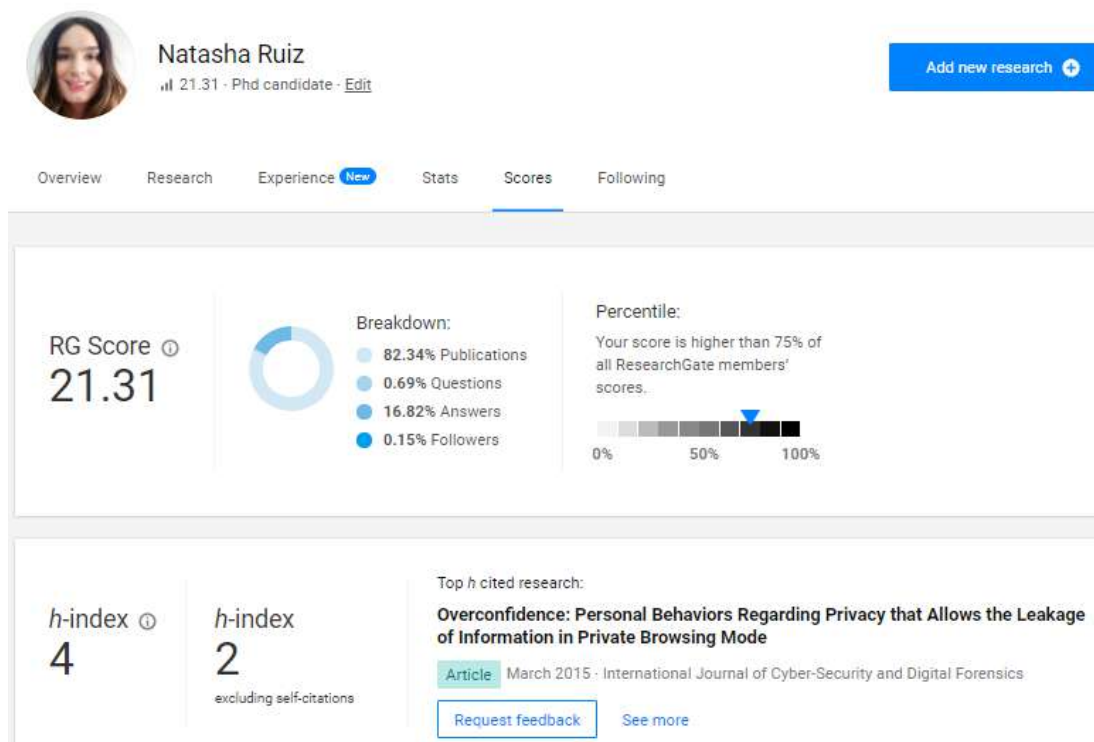


Figure 24 The Researchgate score is indicative of the paper's relevance.

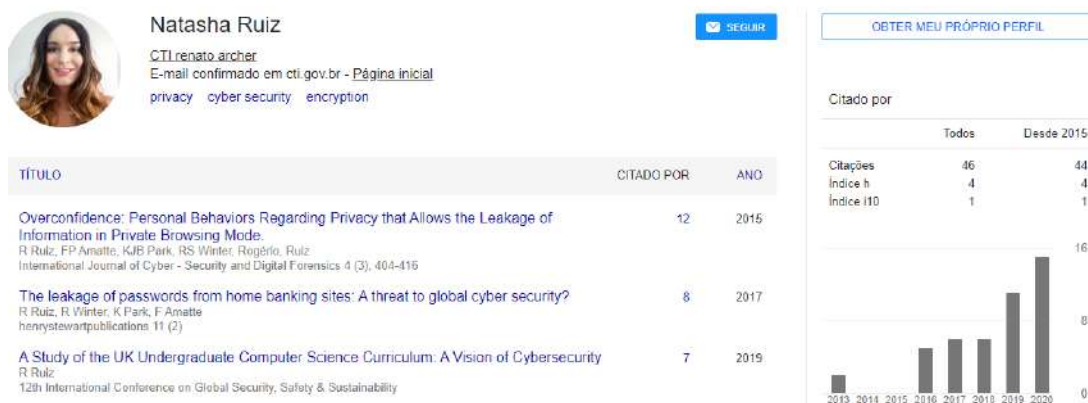


Figure 25 Google Scholar statistics

Appendix B Other Academic and Social Contributions

The peer reviews and these citations, in special citations in a thesis, helps to improve relevance for author's publications during the last ten years, including the entire work of the author. The classic way to measure the relevance of academics is the citations. In this way, the work of the author can prove 60 citations in Researchgate and 42 at Google Scholar with H-index 4 and I10 Index 1. When extracted all self-citations, the number is 22 just for submitted outputs for this thesis.

Another academic contribution is to work as a volunteer at conferences and Journals. I work as a Reviewer for the Journal of Homeland Security and Emergency Management (De Gruyter, 2018). I am Industry Solutions Chair at Second South American International Conference on Industrial Engineering and Operations Management, São Paulo, April 2020. (Anon., 2020)

Below is a list of other publications that do not direct relation that this thesis or are republished work.

Application of the Brazilian anti-malware assessment method and the repercussions for cyber defence (originally published in Portuguese as -Aplicação do método Brasil de avaliação de anti-malware e as repercussões para a defesa cibernética) (Montes, et al., 2014)

The method consists of the following test elements: a) Scan - identify and verify scanning techniques, including file types and extensions. c) Cleaning/removal/quarantine rate is a process that aims to separate the malicious part from the non-malicious part of a file, whereas the removal process aims to delete the file, while the quarantine aims to make an inaccessible file the user or other programs.

e) Installation/update indicators - identify how the product manages its updates, including details of base size and frequency of updates. f) Usability of the software - identify the ease of use of the system and the generation of reports of the system under analysis. g) Stability indicators - identify possible problems related to product stability during use. h) Security indicators - identify possible security flaws that compromise the effectiveness and efficiency of the software.

- Individual contribution: Design of method.

Method and Tool for Generating Table of Relevance, presented at London Metropolitan Conference, April 2020 DOI: 10.13140/RG.2.2.14360.62725 and presented and published by 22 nd European Conference on Knowledge Management ECKM 2021 DOI: 10.34190/EKM.21.199, Coventry University, 2021.

Nowadays, software engineering solutions for supporting the scientific research process are needed. With many articles in thousands of scientific sources, methods to improve and ease the selection and prioritization of research works are demanded, mainly in systematic or quasi-systematic literature reviews. Increase the productivity of software engineering researchers by using structured relevance tables in literature reviews is possible. In this paper, a method and its software tool are presented aiming at generating relevance tables. From the content of the papers (Title, Abstract, etc.), word clouds are generated for selecting and organizing the works, and a heat map based relevance table arises aiming at prioritizing the works to be used in the literature review. The main contributions are i) the method for generating relevance tables in literature reviews (MTTR); ii) a software tool for supporting MTTR. The method and software tool is meant to be useful for researchers who need to organize and prioritize works in comprehensive literature reviews.

Individual contribution: Creation of method for heat map table for literature review, creations of software and write 50% of the paper.

Cyber Mission Operations: A Literature Review (Rogerio Winter et al., 2020)

Besides, a new process used to perform this survey which has some advantages over other processes: objective classification of papers, a significant reduction in execution time, fast visualization of results, fast refinement of research, and validation of relevance of the papers. The main contribution is a quasi-systematic and updated literature review of cyber mission operations, pointing out gaps in the literature and research problems to be addressed by researchers. This work finds the state of art in cyber mission operations and explores the military world to review, classify and comment the most relevant published work in this area.

Individual contribution: Creation of method for heat map table for literature review.

A little about security (originally published in Portuguese as Um pouco sobre segurança) (Ruiz, 2013)

This chapter book that discusses security aspects during ERP software development. In Brazil, is verified by common sense one of the more complex tributary systems at the World and the principal concern of the owner of any small company is the diary sales and the register for the government. Delivery correct reports are the principal objective of all developer. Accuracy is equivalent to business security.

Individual contribution: Unique writer of the chapter.

Who is afraid of the sea monsters? (Ruiz, 2016)

This short opinion paper discusses the fear about Dark web, the symbiosis between fear and the security market and neglect of people in password management. As a result of this short text, I received an invitation to speak at Inside Dark Web November 1st-2nd, 2016 Army Navy Club Washington, DC.

Individual contribution: Unique writer of the article.

Symbiosis and Fear, Evolutionary Benefits of Cyber Security (Ruiz, 2017)

This opinion paper is a criticism about the vendors and professionals of Cyber Security and explores the dubious relations between the fear and the sale of protection. The importance of security is dependent on the existence and criticality of the treat.

Individual contribution: Unique writer of the article.

Brazilian Cyber Security – The Challenge Among Technology, Processes, People And Environment (Rogério Winter et al., 2018)

In this effort, this research present and apply a method to analyse Brazilian government web infrastructure. Method: The development of this study used the following methods: 1.1 Information gathering from Brazilian government domains(federal, state and municipal level); 1.2 To query each government domain to get information about HTTP headers; 1.3 To search for pieces of evidence on open source databases about attacks on Brazilian government domains;1.4 Information gathering from data leaks on the Internet relating to Brazilian government;1.5 To analyse https protocol use in government portals to identify the status of digital certificates.

Individual contribution: Revision and coordination of the working group.

Trigona Honey-Client Technical Comparison Report (Ruiz, 2014)

One of my duties here test software and the result of the test of Trigona that is a medium interaction honeypot deserved full detail. This work proposes a new simple method to verify and compare the results proposed by Trigona. As a means of collecting the artefacts, Trigona presented unsatisfactory due primarily to the final results of the collections and the time for detached analysis.

Individual contribution: Unique writer of the article.

Lazarus: Data Leakage With Cryptographic Systems (Rodrigo Ruiz, 2017)

This is a resume of Lazarus: Data Leakage with PGP and Resurrection of the Revoked User did for US cyber defence public. This text summarizes a method to bypass a cryptographic program, recovering credentials from the deleted user.

Individual contribution: Production of 60% of the text.

Apoc@lypse: O fim do antivírus (Ruiz, et al., 2016)

This book is the translation from English to the Portuguese language of the original book Apoc@lypse: The end of Antivirus (Ruiz, et al., 2015)

Individual contribution: Creation of method of cyber-autoimmune disease, coordination of workgroup, and write 50% of the text.

Reprint: Lazarus: Data Leakage with PGP and Resurrection of the Revoked User (Ruiz & Winter, 2016)

This is a reprint for the military public of the original paper (Ruiz & Winter, 2016)

Individual contribution: Production of 60% of the text.

Brazilian "Car Wash" Task Force: Cyber Security Lessons (Ruiz & Winter, 2017)

Opinion short paper about the correct use of cryptographic systems by criminals. This paper remembers the famous case of a banker that was suspect and use Truecrypt and PGP to protect his alleged illegal business. Neither the Federal Police of Brazil nor the FBI was able to open the files, and the banker ended up acquitted for lack of evidence and procedural flaws. In 2019 in another case, another famous Brazilian businessperson was arrested but data still protected by cryptographic software.

Individual contribution: Production of 60% of the text.

Spying Across Borders in the Age of Email (Ruiz & Winter, 2017).

This Scenario Analysis shows a spy case suffered by author by the UK Ministry of Defence with the collaboration of Microsoft Corp. After the author has a paper classified in the anti-terrorism category of an international conference. After a periodic checks in the log history, improper access to email account as found. After a few months of monitoring and mapping and tracking, the digital steps from Brazil to Redmond, Washington to London in the UK Ministry of Defence building here catalogued. The article contains the official and evasive responses from Microsoft and the British government. They do not confirm and do not deny the allegations.

Individual contribution: Production of 70% of the text, creation of forensic method and conduction of laboratory tests.

Credentials (UN)Management in home banking (Ruiz & Winter, 2017).

This is a resumed version of the paper (Ruiz, et al., 2017) and uses common language to professional programmers' persons.

It is about how as possible to opponent to access credential data of bank account, e-commerce and other web-based systems.

Individual contribution: Production of 60% of the text, creation of forensic method and conduction of laboratory tests.

Is Brazil taking advantage of COVID-19 to promote age and social extermination? (Ruiz, 2020)

It is social criticism of the Brazilian Government after the disastrous pronouncement on the national network on March 24, 2020, the Brazilian president and a good part of his team, leave little doubt that the death of a significant portion of the elderly from the lower classes, could be the solution to social security problems.

Individual contribution: Opinion and full text.

Brazil, the pandemic, the specialization of species and the globalized market (Ruiz & Ganzert, 2020)

E-letter in Science Magazine about specialization risks in Brazil production infrastructure. Existence a specialized species, although it is compensations, it has been shown a risky path and that it increases the chance of extinction. (1) Brazil, decided through its councils and society itself, to focus on being a breadwinner of foods, distributing H₂O to the world. Brazil are one of the major world producers of grains, and do not produce a sole farm machine. Human body natural and nutritious germs are being substituted for transgenic with no taste and without nutrients coming from the exterior. Practically a vassal that plants the seed of the feudal lord.

Individual contribution: Opinion and 50% of the text.

REPRINT: Brazil, the pandemic, the specialization of species and the globalized market (Ruiz & Ganzert, 2020)

Reprint in Critical Infrastructure Review Magazine from the original E-letter in Science Magazine about specialization risks in Brazil production infrastructure.

Individual contribution: Opinion and 50% of the text.

A Consumer-Centric Conceptual Framework for Trust Assessment in Cloud Computing (Balcao, et al., 2019)

A framework to measure customer satisfaction in the cloud market.

Individual contribution: Some parts of the text and validation in calculus.

A Study on Trust Models in Cloud Computing (Balcao, et al., 2020)

Literature review on Trust Models in Cloud Computing.

Individual contribution: Automation of Literature review tabulation.

Um cara, 6 passaportes (A guy with 6 passports) (Rodrigo Ruiz et al., 2019)

A book about genealogy using police and Cyber Security investigations techniques to discover the past.

Individual contribution: 80% of the text.

BinStat - Ferramenta para Reconhecimento de Executáveis Empacotados (Park, et al., 2011)

Tool for recognition of packed executable files

Individual contribution: Automation of process.

BinStat Tool for Recognition of Packed Executables (Park, et al., 2012)

Tool for recognition of packed executable files

Individual contribution: Automation of process.

Balcao, A. F. et al., 2019. A Consumer-centric Conceptual Framework for Trust Assessment in Cloud Computing. Abu Dhabi, s.n.

Balcao, A. F. et al., 2020. A study on Trust Models in Cloud Computing. Las Vegas, s.n.

Rodrigo Ruiz et al., V. G. T. G., 2019. Um Cara, 6 passaportes (A Person, With 6 Passports). Campinas: Clube dos Autores.

Rogério Winter et al., R. R. A. C. B. M., 2018. Brazilian Cyber Security – The Challenge Among Technology, Processes, People And Environment. Critical Infrastructure Protection Review, Volume Spring, pp. 37-44.

Rogério Winter et al., R. R. F. d. F. R. M. J., 2020. Cyber Mission Operations: A Literature Review. Las Vegas, s.n.

Ruiz, R., 2011. Brasil, Patent No. Register number 03654-6/2000 - RPI2122.

Ruiz, R., 2013. Um Pouco Sobre Segurança. In: Sistemas Comerciais. Conceitos Modelagem e Projeto. s.l.:Ciência Moderna.

Ruiz, R., 2014. Trigona Honey-Client Technical Comparison Report. Researchgate.net.

Ruiz, R., 2016. Who is afraid of the sea monsters?. Cyber Warnings E-Magazine, Volume November, pp. 84-85.

Ruiz, R., 2017. NK is the new Iraq?. Cyber Defence Magazine, Volume 6, pp. 109-111.

Ruiz, R., 2017. Symbiosis and Fear, Evolucionary Benefits of Cyber Security. United States Cyber Security Magazine, Volume Spring, pp. 61-62.

Ruiz, R. & Winter, r., 2017. Brazilian "Car Wash" Task Force: Cyber Security

Lessons. Cyber Defence Magazine, Volume 11, pp. 15-16.

Ruiz, R. & Winter, R., 2017. Credentials (UN)Management in home banking. [Online] Available at: <https://securityaffairs.co/wordpress/64699/>

Ruiz, R. & Winter, R., 2017. Spying Across Borders in the Age of Email. 2600 Magazine, Volume 33(4), pp. 18-24.

Ruiz, Natasha; Ganzert Tyler, 2020, Brazil, the pandemic, the specialization of species and the globalized market, Science Magazine online <https://science.sciencemag.org/content/367/6484/1289/tab-e-letters>

Ruiz, Natasha, 2020, Is Brazil taking advantage of COVID-19 to promote age and social extermination?, Science Magazin online <https://science.sciencemag.org/content/343/6168/228.1/tab-e-letters>

Ruiz, Natasha; Shukla, Pancham; Kazemian, Hassan, 2020, Privacy in The First Line of the First Code, Science Magazine online <https://science.sciencemag.org/content/317/5842/1178/tab-e-letters>

Ruiz, Natasha; Shukla, Pancham; Kazemian, Hassan, 2020, UK Cyber Security Index for Undergraduate Computer Science Courses in the UK, 2020, Journal of Applied Security Research

Appendix C: Research Background

The candidate is IT professional since 1992, after 19 years working in the ERP industry, during that time he went from programmer to software engineering team coordinator until I started my own company where he built their software, structured the sales teams and succeeded in satisfying hundreds of companies. My ability to understand the customer business has always put me in a leading position among IT technicians and professionals in the various departments of the companies served.

Actual researcher and former CISO of IT Research Centre for Brazilian Ministry of Science, Technology, Innovations and Communications. He has experience in quality for software development is used in the Cyber Security Division. Since 2011 I'm working in many projects for Brazilian Federal Police, Brazilian Justice and Brazilian Army in fraud investigations, intelligence and software vulnerability and quality. Bringing significant results to the federal public administration, Justice and National Defence, my skills were especially important in reports of public procurement processes for justice software, database analysis and support for the creation of police surveillance software for power and the creation of methodology and laboratory of efficiency tests of antivirus software for the Brazilian Army.

He promotes the introduction of many security, organization and accessibility process in benefit of the institution and was responsible for advising the Director of the Institute and several times assisting the team of the Minister of Science, Technology and Innovation of Brazil.

Support many social programs from the Brazilian Government, my institute and Federal Institute of Education like the internet access for minority groups in

remote locations. Training project and inclusion of graduates of the prison system is launched at IFSP / Campinas.

Actual he is part of Cyber Security Group at DIMEC Division at CTI Renato Archer - Brazilian Ministry of Science.

During the last 10 years, he has been a Cyber Security and genealogy speaker at several relevant events and also for higher education classes.

He has an expert in databases, pattern recognition, data manipulation and vulnerability research. Also consultant and author of genealogy investigations and citizenship process.

Academic life:

2020 – PhD candidate at London Metropolitan University in Computer Science, Scholl of Computing and Digital Media.

2018 – Certificate of post-graduation in Specialist In Cybercrime And Cyber Security: Crime Prevention And Investigation.

2012 – Technologist in Trade Commerce UNINTER University Center

1992 – IT Technician OPET Technical high school

Professional Membership

SDIWC Id 9147

IEEE Id 92902273

Researchgate

Reviewer of a scientific journal (Volunteer)

Reviewer at Journal of Homeland Security and Emergency Management.

Industry Solution Chair of Second South American International Conference on Industrial Engineering and Operations Management, São Paulo, April 2020

Software and patents

ERP Software registered into Brazilian Institute of Intellectual Property INPI as number 03654-6/2000 published into RPI2122 06/Sep/2011

Work Experience:

2011- Today - Brazilian Government Servant at CTI-Renato Archer (Information Technology Center) (IT Research Center of Brazilian Government)

Time life job won in a national public tender.

As a Chief of Security Office, I improve modern security policies in the research centre.

As a Chief of IT, I improve successful new projects like the modern IP phone system, best practices and improve customer satisfaction for 98%.

As Cyber Security Researcher I work at consulting for Brazilian Justice and Brazilian Army (evaluation of compliance purchase of software development, analysis of requirements and effective work of software functions). Considered one of the most relevant researches at the institution (metrics of institution and researchgate.net) the list of publications is presented below.

The research improves more security into the public and private banks, have recognitions of importance by Microsoft Corp and improve the recognition of peers in prestigious conferences.

1999-2009 – Enterprising Consult Ltd. (ERP Company)

Responsible to design the ERP database and business rules for major of

software, I always coordinate the software deployment and client satisfaction. More than 100 clients with success stories.

Understanding and paying particular attention to the needs and peculiarities of each client, considering the technological, social and business resources involved in each request, always guarantee the best result and satisfaction generating customer satisfaction.

1994-1998 – Totvs (Major ERP Company of South America)

In this biggest Software company of South America, I develop in Clipper based language to promote customizations in ERP software. Hundreds of client preferred to call me to the detriment of other professionals both for my knowledge and tact as for the commitment to the client.

In addition to coordinating an ERP deployment team, I was primarily responsible for internal support for other consultants in reporting on tools such as Crystal Reports and the development of complex SQL queries.

Others courses

2011 – Counter-Intelligence at Prospect Intelligence

2012 – Theory of discourse at UNICAMP (University of Campinas)


2013 – Forensic Research at CTI – Renato Archer

2019 – Course of Python for Research at HarvardX

2019 – Entrepreneurship at University of Barcelona

Appendix D: Specialist Diploma


REPÚBLICA FEDERATIVA DO BRASIL
 REPUBLIC OF BRAZIL




REPÚBLICA FEDERATIVA DO BRASIL
 FEDERATIVE REPUBLIC OF BRAZIL
 ESTADO DE PERNAMBUCO/STATE OF PERNAMBUCO
 ANTONIO DARI ANTUNES ZHBANOVA
 TRADUTOR PÚBLICO E INTÉRPRETE COMERCIAL - CERTIFIED PUBLIC TRANSLATOR
 Idioma/Language: Inglês - Português/English - Portuguese
 Matrícula Jucepe nº 406 - CPF 756.770.758-68
 Rua Princesa Isabel nº 206 - Aloisio Pinto - Garanhuns (PE) CEP: 55.292-210
 Telefone/Phone/What's app +55 87 99954-2519 - e-mail: dari.zhbanova@gmail.com (skype: antonio.dari)

TRADUÇÃO Nº	LIVRO Nº	FOLHA Nº
TRANSLATION No.	BOOK No.	PAGE No.
5384	030	01

The undersigned, certified public translator, duly sworn and registered with the board of trade of the state of Pernambuco under no. 406 hereby certifies that a document, written in Portuguese, was presented for translation into English, which has been done to the best of his knowledge as follows:



Faculdade Cidade Verde
Maringá – Paraná



CERTIFICATE
“Lato Sensu” Post-Graduation

The General Director of Faculdade Cidade Verde confers the Specialist Degree to

Rodrigo de Souza Ruiz

for the conclusion of the Post-Graduation course in **Cybercrime and Cybersecurity: Prevention and Investigation of Digital Crimes**, Specialization level, with **420 class hours**, approved by the Board of Directors through the Resolution n. 003/16, dated Mar/10/2016, and promoted by this College in the period from January 2018 to June 2018.

Maringá, June 29th, 2018.

[Illegible signature]
Prof. Spec. Magda Maria
Fernandes
Academic Affairs
Coordinator

[Illegible signature]
Prof. Ms. Valdemar Dias dos
Santos
Graduation, Post-Graduation
and Extension Director

[Illegible signature]
Prof. Dr. Hamilton Luiz
Favero
General Director

[On the verse:]

Student: Rodrigo de Souza Ruiz

Course: Cybercrime and Cybersecurity: Prevention and Investigation of Digital Crimes

Knowledge Field (CAPES/CNPQ): Management and Business

CPF [Individual Taxpayer Number]:
864.456.189/87

Registry n.: 477

Registry Date: Jun/29/2018

Book: Page:
1 48

INSCRIÇÕES/REGISTRATIONS:

RG [Id Card] 8.489.091-5

CPF 756.770.758-68

JUCEPE nº 406



REPÚBLICA FEDERATIVA DO BRASIL
FEDERATIVE REPUBLIC OF BRAZIL
ESTADO DE PERNAMBUCO/STATE OF PERNAMBUCO
ANTONIO DARI ANTUNES ZHBANOVA

TRADUTOR PÚBLICO E INTÉRPRETE COMERCIAL - CERTIFIED PUBLIC TRANSLATOR
Idioma/Language: Inglês - Português/English - Portuguese
Matrícula Jucape nº 406 - CPF 756.770.758-68

Rua Princesa Isabel nº 206 - Aloisio Pinto - Garanhuns (PE) CEP: 55.292-210
Telefone/Phone/What's app +55 87 99954-2519 - e-mail: dari.zhbanova@gmail.com (skype: antonio.dari)

TRADUÇÃO Nº 5384 LIVRO Nº 030 FOLHA Nº 02
TRANSLATION No. BOOK No. PAGE No.

Subject	Professor	Title	WL	Grade	Attendance	Final Situation
Cybernetic Crimes and Intelligence	Maurício Pessoa Gebran	Master	80	9.0	100%	Approved
Cybercrime, Cybersecurity and Police Intelligence	Maurício Pessoa Gebran	Master	80	8.5	100%	Approved
Strategic and Organizational Management	Márcia Huppe Fávero	Specialist	60	8.0	100%	Approved
Introduction to Web Programming	Daniilo Sartorelli Barbato	Specialist	60	9.0	100%	Approved
Ethics and Social and Professional Responsibility	Oswaldo Oliveira Santos Júnior	Master	60	7.0	100%	Approved
Research and Scientific Work Methodology	Hugo Allan Matos	Master	60	8.0	100%	Approved
Final Paper	Hugo Allan Matos	Master	20	9.0	100%	Approved
Final Paper Title: "D.O.S. Attacks in critical infrastructure using social network." Professor Advisor: Adival José Reinert Junior				9.0	Approved	

Accredited by Ordinance n. 1.721, of May/19/2005, published on the Official Gazette on May/20/2005. Reaccredited by Ordinance n. 1.535, of Oct/24/2011, published on the Official Gazette on Oct/25/2011. Accredited in Distance Education by Ordinance n. 635, of May/17/2017, published on the Official Gazette on May/18/2017. This Course complied with all provisions of the CNE/CES Resolution n. 1 of April 06th, 2018.

Maringá, June 29th, 2018.

FCV – Faculdade Cidade Verde – Av. Adv. Horácio Raccanello Filho, 5950 – Zona 01 – Zip Code: 87020-035
Maringá – Paraná – Telefax: (44) 3028-4416
CNPJ [Corporate Taxpayer Number]: 05.885.457/0001-44



REPÚBLICA FEDERATIVA DO BRASIL
FEDERATIVE REPUBLIC OF BRAZIL
ESTADO DE PERNAMBUCO/STATE OF PERNAMBUCO
ANTONIO DARI ANTUNES ZHBANOVA

TRADUTOR PÚBLICO E INTÉRPRETE COMERCIAL - CERTIFIED PUBLIC TRANSLATOR
Idioma/Language: Inglês - Português/English - Portuguese

Matricula Jucepe nº 406 - CPF 756.770.758-68

Rua Princesa Isabel nº 206 - Aloisio Pinto - Garanhuns (PE) CEP: 55.292-210
Telefone/Phone/What's app +55 87 99954-2519 - e-mail: dari.zhbanova@gmail.com (skype: antonio.dari)

TRADUÇÃO Nº	LIVRO Nº	FOLHA Nº
TRANSLATION No.	BOOK No.	PAGE No.
5384	030	03

This translation does not imply any judgment on the form, authenticity and/or contents of the translated document. Nothing else in the document, which I have faithfully translated into English. In witness thereof, I set my hand and seal on this eighth day of August of two thousand and eighteen, in the city of São Paulo – state of São Paulo

Emoluments according to the law.

São Paulo, August 08th, 2018

Antonio Dari Antunes Zhbanova
Tradutor Público/Public Translator



Appendix E: Recommendation Letter, Professor

Abdul Razaque



New York Institute of Technology
School of Engineering

Department of Computer Science

Abdul Razaque, Ph.D.
Associate Professor
New York, USA
Tel: +1-3474848598
E-mail:
arazaque@nyit.edu

Recommendation letter for Rodrigo Ruiz

It is my great pleasure to write this letter in support of Rodrigo de Souza Ruiz. As, Ruiz research was focused on one critically cyber security issues and business intelligence development.

Rodrigo Ruiz is an outstanding and exceptionally skilled scientist whose groundbreaking research work is of vital importance to our country's defense in national scope. His accomplishments to date have far exceeded those of most of his peers as evidenced by his productive publications in premier scientific journals and frequent citations of his works by other researchers.

Rodrigo Ruiz research work aims to tackle the problems of credential management especially in cryptographic containers and web systems. What we learned from his research project is critically important for development and application of new methods of security and defense.

I feel fortunate to have had Rodrigo Ruiz in my academic relations. His research works are wellrecognized nationally. Rodrigo Ruiz significant accomplishments are far above what is expected from his peer group and have established him as a nationally and internationally outstanding researcher in the field of cyber security and business intelligence. His research is doubtlessly in the national interest. I believe that Rodrigo Ruiz will be very productive in his research efforts.

Sincerely,

Abdul Razaque, PhD

Appendix F: Recommendation Letter, Dr Mauro Coimbra

RECOMMENDATION LETTER

To whom it may concern

Mr. **Rodrigo de Souza Ruiz** is someone particularly easy to recommend, for his unique personal and professional traits. Besides his very solid background in I.T at large, with emphasis in Security concepts and techniques, he is a very creative professional, always trying to think out of the box — something that is especially critical for I.T Security. He has a keen business acumen and negotiation skills developed when working in a very distinguish consultancy company in Brazil.

To conclude, he is always open to learn new things and reinvent himself aiming at being always abreast with new concepts, technologies and contexts — having an unflagging spirit of self-teaching, despite his great teamwork personality.

Please do not hesitate to contact me should you need any additional information.

Respectfully,


Mauro de Lima Coimbra
mauro.coimbra@lecti.com.br

Short résumé: Dr. Coimbra is a seasoned I.T. professional, with more than 35 years of experience working for private and public national and international companies. His professional background as a research engineer and technical has been developed building, coaching, and managing all dimensions of small and large multidisciplinary teams (in excess of 300 people) for major projects — from system and hardware design, to deployment and operation of comprehensive Telecommunications, Information Technology, Plant Automation and Tolling systems & infrastructure. Experienced in commercial and top management negotiations between companies and with the Brazilian Government Agencies, whenever occupying top management positions (V.P. or Director). He's got a Ph.D. degree in Electrical Engineering (Telecommunications/Electronics), 1996; MBA-Executive, 1994; M.Sc. in Electrical Engineering, 1981; B.Sc in Electronics and B.Sc in Telecommunications both in 1978. He is also an Attorney at Law, under professional license OAB/SP-376.815, since Dec. 2015, as a Public Defender, to the less economically favoured people, thanks to an agreement between OAB/SP and the State of São Paulo, Brazil.

Campinas, September 21st, 2018
São Paulo, Brazil

Appendix G: Recommendation Letter, Dr Jarbas Cardoso

Campinas, September 6th, 2018

To whom it concerns.

I am pleased to recommend Mr. Rodrigo de Souza Ruiz for conducting research at your institute on topics related to his expertise in information security.

I happened to know Ruiz in the year 2010, when he started to work at the Center for Information Technology Renato Archer (CTI), a research unit of the Ministry of Science, Technology, Innovation and Communications (MCTIC) of the Brazilian government. Very fast, he got the position of computer support manager of CTI with the mission to manage IT resources to support the research activities and the security issues related to IT operation. We have worked together in activities related to IT strategic planning for the CTI. Since I know him, he was proved to be a very interested researcher, collaborating and facing new challenges to meet public policies for science, technology and innovation.

Mr. Ruiz has remarkable background in the cyber security domain. As IT manager, he has provided an efficient, security, and reliable IT support for CTI's research activities. As a researcher, he has strong scientific interest in learning and has published important papers and a book. So, I feel very comfortable to recommend Mr. Ruiz to conduct research in your institute.

Please do not hesitate to contact me with regards to any further information you might need on his qualifications.

Sincerely


Jarbas L. Cardoso Jr.
<http://lattes.cnpq.br/3089352247066003> (detailed CV)
https://www.researchgate.net/profile/Jarbas_Cardoso_Junior

Short Resume. Jarbas Lopes Cardoso Jr. has worked for the Center for Information Technology Renato Archer (CTI), Brazil, since 1984. He is a senior scientist and as software project manager, he has conducted several projects carried out in collaboration with national and international public and private institutions. In his first international experience, he coordinated a work-package of the Electronic Government Innovation and Access Project (eGOIA), a European Union funded initiative of Alliance of Information Society (@lis). He has recently managed two projects related to Brazilian Science and Technology policy: "Reference Model for Brazilian Public Software" and "Middleware Ginga Evaluation" (Brazilian standard for Digital TV). As a university professor, he has taught classes in undergraduate courses of Computer Science and Information Systems at PUC-Campinas and UNIP-Campinas, and MBA in IT Governance at UNICAMP and at National School of Networks (ESR). He received the PhD degree from the Polytechnic School, University of Sao Paulo (USP). Part of his research activities during his doctorate was carried out in National Institute of Informatics (NII), Japan, and at Kasetsart University (KU), Thailand. He has published books and papers in journals and conference proceedings. His research areas of interest are: collective intelligence, problem-solving by cases, collaborative innovation networks, and social project management. He is member of the Institute of Electrical and Electronics Engineers (IEEE) and Brazilian Computer Society (SBC/ACM-Brazil). Written by him, the book "Collective Intelligence - Decision Support in Collaborative Environments" was released last January (2018) - <https://www.morebooks.de/store/pt/book/intelig%C3%Aancia-coletiva/isbn/978-620-2-03946-8>.

Appendix H: Recommendation Letter, Dr Ferruccio

Rosa

Professional Recommendation Letter

I would like to introduce Rodrigo de Souza Ruiz. Mr. Ruiz is a public servant from the Brazilian Government, since 2010.

Regarding professional skills and research activities. Ruiz is currently managing the Computational Infrastructure Division in our institution, but he can adapt himself to deal with other activities and issues related to systems administration and security. He deals with credential management issues, especially in cryptographic containers, and anonymous browsing on Web systems. This research, in the cyber security area, is important for the protection of governmental systems and networks. The research developed by Ruiz has obtained important results, such as scientific articles and technical reports.

Regarding personal characteristics. Ruiz is a serious professional, result-oriented and good co-worker. He is easy to work with; he listens, learns, and gives clear feedbacks. He is a motivated professional and has a promising future in the Security Information domain.

I believe professionals with skills in Cyber Defense are important for any country, especially for USA. Therefore, I recommend that the Rodrigo Ruiz's work request be granted.



Ferruccio de Franco Rosa

Ferruccio de Franco Rosa received the Ph.D. degree in Electric Engineering at the Campinas University, Brazil. He is a Senior Researcher with the Aeronautic Command (Brazilian Air Force), working in the Ministry of Science and Technology. He has experience on software assessment with emphasis on finding security defects. From 2012 to 2015 he was Head of the Information Systems Security Division (DSSI) at the Center for Information Technology Renato Archer (CTI). Dr. Rosa lead the research project "Information Systems Security" (#PRJ04.35) that aims to propose systematic methods for generating better sets of security assessment items based on the coverage of security properties and assessment dimensions.

Appendix I: Recommendation Letter, SDIWC



The Society of Digital Information and Wireless Communications (SDIWC)

20/F, Tower 5, China Hong Kong City, 33 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong

To whom it may concern,

It's my pleasure to recommend the academic work of Rodrigo Ruiz, a member of The Society of Digital Information and Wireless Communications (SDIWC) and active collaborator for the development and studies of global cyber security and privacy.

His work is modern and actual and was peer-reviewed and represent important contribution to The Society of Digital Information and Wireless Communications (SDIWC) , companies, governments and society.

Papers published in International Conferences and journals:


- Private Browsing " Data - Acquiring Evidence of Browsing Activities published at **The International Conference on Information Security and Cyber Forensics (InfoSec2014)**
- Security Issue on Cloned True Crypt Containers and Backup Headers -published at **The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)**
- Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode into International published at **Journal of Cyber Security and Digital Forensics**
- Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life **International Journal of Cyber Security and Digital Forensics Vol. 7, 1**

Sincerely yours,

Liezelle Ann Canadilla

SDIWC office

Appendix K: Recommendation Letter, Bob Miko

Memo 23-Jul-19		Pacific Dialogue Trade Show Bureau, 33280 East Nimrod, Solon OH 44139 USA Bob Miko, Public Relations Director Tel: 203-378-2803 bmiko@pacificdialogue.com www.pacificdialogue.com
--------------------------	---	--

Professional Recommendation for Rodrigo Ruiz (full name Rodrigo de Souza Ruiz)

Mr Ruiz is an experienced published author with a 25 year long career in Information Technology and Cybersecurity. He has authored more than 20 professional journal and magazine articles related to Cybersecurity, the Dark Web and technology.

He assisted my organization in presenting our two day conference Inside the Dark Web to the Brazilian government Cybersecurity training center. He is also Brazilian Government Servant at CTI-Renato Archer (Information Technology Center) (IT Research Center of Brazilian Government) the equivalent of the American Law Enforcement Cyber Training Center sector of Homeland Security.

Mr. Ruiz is currently pursuing his Doctor from the Dublin Institute of Technology which he expects to complete in 2019.

Mr Ruiz holds Professional memberships in:

- SDIWC Id 9147
- IEEE Id 92902273
- Researchgate

Of course Mr Ruiz is a native Brazilian speaker with an working understanding of Spanish and is fluent in English (having written a number of his publications in English).

It is an honor to recommend him for any position that he would apply for.

Robert J. Miko

Robert J. Miko
Founder & CEO
Pacific Dialogue Trade Show Bureau

Appendix L: Recommendation Letter, Julia Dolengo



DELTA BUSINESS MEDIA LIMITED

Print, digital and online specialist publisher

31 August 2018

To whom it may concern,

Dear Sir/Madam

I had a great opportunity to work closely with Mr Rodrigo Ruiz since 2016. During these years we had collaborated on two projects, and I am pleased to say that Rodrigo is an excellent team player, sincere and hardworking individual who always meet his deadlines and happy to face challenging tasks at hand.

His academic work published in our magazines 'Cyber Security Review' and 'Critical Infrastructure Protection Review' includes:

- 2016 'Corrosive Secrecy And Confidence: The Paradox Among Bypassing Cryptographic Software, Loss Of Privacy And Information Security' - published in Cyber Security Review magazine
- 2016 'Apocalypse: The End Of Antivirus. When The Antivirus Is The Threat' - published in Cyber Security Review magazine
- 2017 'Lazarus: Data Leakage with PGP and Resurrection of the Revoked User' - published in Cyber Security Review magazine
- 2017 'Cybersecurity, Cyber Weapons And Cyber-Attacks: Responsibility And Different Reflections On The Subject' - published in Critical Infrastructure Protection Review magazine
- 2018 'Brazilian Cybersecurity – The Challenge Among Technology, Processes, People And Environment' - published in Critical Infrastructure Protection Review magazine.

I am glad to have worked with Rodrigo and highly recommend him for a suitable position he may decide to apply. He is a very talented person who has a comprehensive knowledge and skills to deal with the vast range of cyber security challenges, and I wish him all the best in his future endeavors.

Yours faithfully

Julia Dolengo

Publisher – 'Cyber Security Review' and 'Critical Infrastructure Protection Review' magazines

Delta Business Media

3rd Floor, 207 Regent Street | London, W1B 3HH | United Kingdom

Tel: +44 (0) 20 7193 2303 | Fax: +44 (0) 203 014 7659

Email: jd@deltabusinessmedia.com

Delta Business Media Limited, 3rd Floor, 207 Regent Street, London W1B 3HH, United Kingdom
Tel: +44 (0) 207 193 2303 | Fax: +44 (0) 20 3014 7659 | info@deltabusinessmedia.com | www.deltabusinessmedia.com
Registered in England, Company No. 7973076 | VAT No. 131810550

Appendix M: Recommendation Letter, Lorival Moreira



SERVIÇO PÚBLICO FEDERAL
MSP - DEPARTAMENTO DE POLÍCIA FEDERAL
SR/SP - DELEGACIA DE POLÍCIA FEDERAL EM CAMPINAS
NÚCLEO TÉCNICO-CIENTÍFICO


Recommendation Letter

It's my pleasure to write this letter to recommend Rodrigo Ruiz.

Mr. Ruiz is currently CISO of a Brazilian Federal Research Institute, CTI-Renato Archer and coordinator of Superior School of Networks from National Research Network. He works closely with the Federal Police in surveillance projects like Oráculo and Colossus. He conduct researches about privacy and credential management that contribute to turn the cyber world more secure, especially in cryptography and data carving.

As personal goals, Ruiz is a loyal colleague and a motivated professional. He is easy to work and he use direct and clear communication.


I believe that Mr. Ruiz bring important contributions to Brazil and global cyber security and certainly he will contribute to US in the cyber security and software field.



LORIVAL CAMPOS MOREIRA
PERITO CRIMINAL FEDERAL
Chefe do NUTEC/DPF/CAS/SP

Lorival Campos Moreira holds a degree in Systems Analysis from the Pontifical Catholic University of Campinas (PUCCAMP), holds a Specialization in Psychopedagogy from the Federal University of Rio de Janeiro (UFRJ) and holds a Master of Business Administration (MBA) Degree in Management Excellence with an Emphasis on Public Administration from Fundação Armando Alvares Penteado - FAAP. Sergeant of the Brazilian Army for 20 years and currently is Agent of Brazilian Federal Police, in the position of Expert in Federal Crimes, serving as Chief of the Technical-Scientific Nucleus (Nucleus of Expertise) of the Federal Police Station in Campinas, SP.

Appendix N: Invitation to Keynote Speaker

Memo		Pacific Dialogue Trade Show Bureau, 33280 East Nimrod, Solon OH 44139 USA
		Bob Miko, Event Producer & Director Tel: 203-378-2803 bmiko@pacificdialogue.com www.pacificdialogue.com
18 October 2016		

Invitation to Keynote
Inside the Dark Web,
November 1-2, 2017,
Army Navy Club, Washington, DC

Mr. Rodrigo Ruiz
CTI Brazil
Information Technology Center
Renato Archer, Campinas, Brazil

Dear Mr Ruiz

This is your formal invitation to be one of our keynote speakers at the upcoming Inside Dark Web Conference, November 1-2 in Washington, DC.

We would be honored for you to provide an international perspective on this global networking issue. We have speakers from various US Government agencies and the private sector and we greatly appreciate your willingness to give us an international point of view.

As I have mentioned and you will find on our website, Insidedarkweb.com, the focus of our two day conference is what the business and private sector must do to deal with the dark web in partnership with many governmental organizations. The dark web is both a concern but also is a benefit and the balance of how to use it is what we will be presenting at this event.

Thank you for your interest in helping us provide a forum for the discussion of this challenging issue.

Sincerest regards

Robert J. Miko
Robert J. Miko
Producer
InsideDarkWeb

Appendix O: Invitation to Comment on Cyber Security to International Media

De: Michelle Kuepper <michelle.kuepper@researchgate.net>

Enviado: sexta-feira, 30 de junho de 2017 07:22

Para: rodrigossruiz@outlook.com

Assunto: Press enquiry

Hi Rodrigo,

My name is Michelle and I work in communications at ResearchGate. I'm getting in touch as I have received a media enquiry from a Washington Post journalist in regards to the recent cyberattack. He's looking for

webmail.cti.gov.br/zimbra/f/printmessage?id=32508&tz=America/Sao_Paulo

1

2020

Zimbra

expert input on the following questions:

1. Who's behind this NonPetya malware (not ransomware, but malware that overwrites data in your network) that targeted Ukrainian banks, energy firms, etc.?
2. Is this a diversionary attack to mask something more sinister?
3. Any traces to any particular Russian spy agency?

Is this something you can speak to? I realize these are the exact questions cybersecurity experts are asking themselves, but I imagine the journalist would also be interested in an expert perspective on them even if there are no definitive answers. Would you be able to provide a short response we can forward, and can we offer to put him in touch with you if he'd like to talk more?

To provide more context, here is the follow-up email the journalist sent me:

There is a Reuters report now that says another Ukraine company has been hit with a new virus. What Ukrainian cyber security experts have said is that the virus was timed to hit on the eve of their Constitution Day, and that there was no ransom effort. They are also saying that certain systems on the "gray internet" -- Tor, certain VPN -- were used that are advertised in Russian social media. Apparently these systems had been banned by Ukraine's cyber watchdog, and anyone who avoided them was unaffected in the attack. That's the evidence they've offered so far for why they think this is a tactic of Russia's hybrid war. I wonder what sober, third-party analysts think about all this.

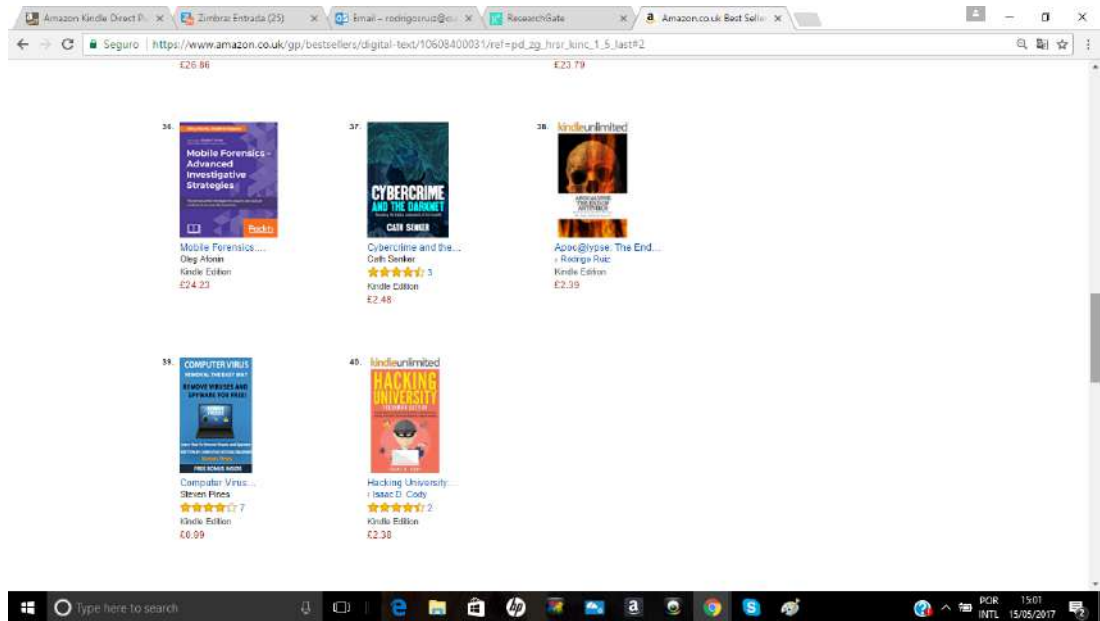
Looking forward to hearing from you!

Best,
Michelle

Michelle Kuepper
Public Relations Manager

ResearchGate GmbH

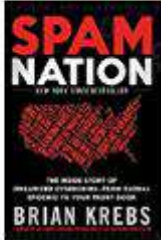





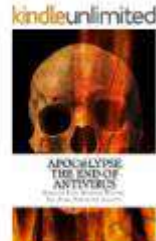

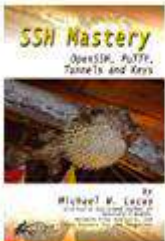
Appendix P: Amazon top 100 UK (Ruiz, et al., 2015)



Appendix Q: Amazon top 10 Germany (Ruiz, et al., 2015)

guro | https://www.amazon.de/gp/bestsellers/digital-text/646435031/ref=pd_zg_hrsr_ki

Top 100 Top 100 gratis

<p>1. </p> <p>Spam Nation: The... Brian Krebs ★★★★★ 3 Kindle Edition EUR 7,99</p>	<p>2. </p> <p>TOR: Exactly How to... Joshua Cody Kindle Edition EUR 2,99</p>	<p>3. </p> <p>The Hacker Playbook 2: ... Peter Kim ★★★★★ 1 Kindle Edition EUR 13,20</p>
<p>4. </p> <p>Black Hat Python: ... Justin Seitz Kindle Edition EUR 15,99</p>	<p>5. </p> <p>Hacking Wireless... Andreas Kolokithas ★★★★★ 1 Kindle Edition EUR 17,38</p>	<p>6. </p> <p>Implementing... Richard M. Hicks ★★★★★ 1 Kindle Edition EUR 41,19</p>
<p>7. </p> <p>Apoc@lypse: The End... Justin Seitz</p>	<p>8. </p> <p>Mastering Bitcoin: ... Andreas M. Antonopoulos</p>	<p>9. </p> <p>SSH Mastery: ... Michael W. Lucas</p>

Appendix R: Invitation to Publish a Book

Publication of your book based on "The leakage of passwords from home banking sites: A threat to global cyber security?"

AT Ana-Maria Tihon <a.tihon@lap-publishing.com>
Qui, 07/12/2017 10:15
Para: Você

Dear Rodrigo Ruiz,


I am Ana-Maria Tihon from OmniScriptum Publishing Group.



We would be interested to publish a printed book based on your research entitled "The leakage of passwords from home banking sites: A threat to global cyber security?".


In brief, OmniScriptum is dedicated to scientific works written in English. Our books are distributed worldwide through well known shops such as Amazon, Morebooks, Barnes & Nobles. In addition, we bear all costs related to the production, marketing and distribution of our books.



Rodrigo Ruiz, would you agree to receive more information?

I am looking forward to your reply.


 Sincere regards,
Ana-Maria Tihon
Editor
e: a.tihon@lap-publishing.com
w: www.lap-publishing.com



 **LAMBERT**
Academic Publishing

  Redeem the code xmas_17
and get 10% off on each purchased book at:
www.morebooks.de

Appendix S: Chair of International Conference



Industrial Engineering & Operations Management
São Paulo, Brazil, April 6 – 8, 2021
Venue: Maksoud Plaza Hotel, São Paulo



Home Authors Competitions Registration Program Committee Keynote Global Engineering Education Industry 4.0 Panels Sponsors Travel

» Committee

Committee

Conference Committee

Honorary Chair

- Professor Paulo Roberto Freitas de Carvalho, Director, FACENS University, Sorocaba, Sao Paulo, Brazil

Conference Chairs

- Prof. Vitor M. Caldana, IFSP – Instituto Federal de São Paulo – Campus Sorocaba, SP, Brazil
- Prof. Dr. José Lázaro Ferraz, Coordinator of Production Engineering, FACENS University, Sorocaba, Sao Paulo, Brazil
- Dr. Ahad Ali, Lawrence Technological University, Michigan, USA

Global Engineering Education Chairs

- Ricardo Alexandre Diogo, Professor Adjunto, PUCPR – Pontifícia Universidade Católica do Paraná, Curitiba, Paraná, Brazil

Industry Solutions Chairs

- Rodrigo Ruiz, CTI Renato Archer, Campinas, Brazil

Appendix T: Declarations of Co-writers

STATEMENT OF AUTHORSHIP OF PUBLICATION

On behalf of (Rodrigo de Souza Ruiz)

By (Kil Jin Brandini Park)

I am registering for a PhD by Existing Published or Creative works. A condition of the registration is that I have a statement from collaborating authors confirming the contribution made by myself to jointly authored work. In our case the work is:

Insert details of publication(s)

2017 - The leakage of passwords from home banking sites: A threat to global cyber security?
Rodrigo Ruiz, Rogério Winter, Kil Jin Brandini Park, Fernando Amatte
<https://www.henrystewartpublications.com/jps/v11>

2016- Lazarus: Data Leakage with PGP and Resurrection of the Revoked User
Journal of Cyber Security and Mobility
Rodrigo Ruiz, Rogério Winter
http://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/5/2/1

2015 - Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc., Rogério Winter/Journal Name: International Journal of Cyber-Security and Digital Forensics (JCSDF)
DOI: <http://dx.doi.org/10.17781/P001619>
<http://sdiwc.net/digital-library/overconfidence-personal-behaviors-regarding-privacy-that-allows-the-leakage-of-information-in-private-browsing-mode>

2014 - SECURITY ISSUE ON CLONED TRUECRYPT CONTAINERS AND BACKUP HEADERS
The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
<http://sdiwc.net/digital-library/security-issue-on-cloned-truecrypt-containers-and-backup-headers.html>

2014 - OPENING THE "PRIVATE BROWSING" DATA - ACQUIRING EVIDENCE OF BROWSING ACTIVITIES
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
Conference Name: The International Conference on Information Security and Cyber Forensics (InfoSec2014) Malaysia
2012 - Making the "In Private" Navigation as Public (Tornando Pública a Navegação "In Private") Portuguese
ICCYBER 2011

Rodrigo de S. Ruiz 1, Fernando Pompeo Amatte 2, Kil Jin Brandini Park D. Sc.
DOI: 10.5769/C2012011 or <http://dx.doi.org/10.5769/C2012011>

<http://livrozilla.com/doc/606538/icoics-2011.indd---the-international-conference-on-forensic>

I would be grateful if you would supply the percentage of work in that article that is attributable to me by completing and signing the following statement.

I confirm that (Rodrigo Ruiz) contributed 60 % to the above publication(s).

Signature [Signature]

Date OCTOBER 3, 2017

STATEMENT OF AUTHORSHIP OF PUBLICATION

On behalf of (Rodrigo de Souza Ruiz)

By Fernando Amatte

I am registering for a PhD by Existing Published or Creative works. A condition of the registration is that I have a statement from collaborating authors confirming the contribution made by myself to jointly authored work. In our case the work is:

Insert details of publication(s)

2017 - The leakage of passwords from home banking sites: A threat to global cyber security?
Rodrigo Ruiz, Rogério Winter, Kil Jin Brandini Park, Fernando Amatte
<https://www.henrysstewartpublications.com/jps/v11>

2016 - Lazarus: Data Leakage with PGP and Resurrection of the Revoked User
Journal of Cyber Security and Mobility
Rodrigo Ruiz, Rogério Winter
http://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/5/2/1

2015 - Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc., Rogério Winter
Journal Name: International Journal of Cyber-Security and Digital Forensics (UCSDF)
DOI: <http://dx.doi.org/10.17781/P001619>
<http://sdiwc.net/digital-library/overconfidence-personal-behaviors-regarding-privacy-that-allows-the-leakage-of-information-in-private-browsing-mode>

2014 - SECURITY ISSUE ON CLONED TRUECRYPT CONTAINERS AND BACKUP HEADERS
The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
<http://sdiwc.net/digital-library/security-issue-on-cloned-truecrypt-containers-and-backup-headers.html>

2014 - OPENING THE "PRIVATE BROWSING" DATA - ACQUIRING EVIDENCE OF BROWSING ACTIVITIES
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
Conference Name: The International Conference on Information Security and Cyber Forensics (InfoSec2014) Malaysia
2012 - Making the "In Private" Navigation as Public (Tornando Pública a Navegação "In Private") Portuguese
ICCYBER 2011

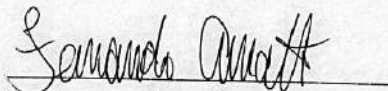
Rodrigo de S. Ruiz 1, Fernando Pompeo Amatte 2, Kil Jin Brandini Park D. Sc.
DOI: 10.5769/C2012011 or <http://dx.doi.org/10.5769/C2012011>

<http://livrozilla.com/doc/606538/icofoes-2011.indd---the-international-conference-on-forensic>

I would be grateful if you would supply the percentage of work in that article that is attributable to me by completing and signing the following statement.

I confirm that (Rodrigo Ruiz) contributed 60 % to the above publication(s).

Signature



Date

06 June 2018

STATEMENT OF AUTHORSHIP OF PUBLICATION

On behalf of (Rodrigo de Souza Ruiz)

By (Rogério Winter)

I am registering for a PhD by Existing Published or Creative works. A condition of the registration is that I have a statement from collaborating authors confirming the contribution made by myself to jointly authored work. In our case the work is:

Insert details of publication(s)

2017 - The leakage of passwords from home banking sites: A threat to global cyber security?
Rodrigo Ruiz, Rogério Winter, Kil Jin Brandini Park, Fernando Amatte
<https://www.henrystewartpublications.com/jpss/v11>

2016 - Lazarus: Data Leakage with PGP and Resurrection of the Revoked User
Journal of Cyber Security and Mobility
Rodrigo Ruiz, Rogério Winter
http://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/5/2/1

2015 - Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc., Rogério Winter
Journal Name: International Journal of Cyber-Security and Digital Forensics (IJCSDf)
DOI: <http://dx.doi.org/10.17781/IJ001619>
<http://sdiwc.net/digital-library/overconfidence-personal-behaviors-regarding-privacy-that-allows-the-leakage-of-information-in-private-browsing-mode>

2014 - SECURITY ISSUE ON CLONED TRUECRYPT CONTAINERS AND BACKUP HEADERS
The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
<http://sdiwc.net/digital-library/security-issue-on-cloned-truecrypt-containers-and-backup-headers.html>

2014 - OPENING THE "PRIVATE BROWSING" DATA - ACQUIRING EVIDENCE OF BROWSING ACTIVITIES
Rodrigo de S. Ruiz, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc.
Conference Name: The International Conference on Information Security and Cyber Forensics (InfoSec2014) Malaysia

2012 - Making the "In Private" Navigation as Public (Tornando Pública a Navegação "In Private") Portuguese
ICCYBER 2011
Rodrigo de S. Ruiz 1, Fernando Pompeo Amatte 2, Kil Jin Brandini Park D. Sc.
DOI: 10.5769/C2012011 or <http://dx.doi.org/10.5769/C2012011>

<http://livrozila.com/doc/606538/icoecs-2011.indd---the-international-conference-on-forensic>

I would be grateful if you would supply the percentage of work in that article that is attributable to me by completing and signing the following statement.

I confirm that (Rodrigo Ruiz) contributed 100 % to the above publication(s).

Signature  ROGERIO WINTER

Date OCTOBER 02 2017

Appendix U: Full Text of Prior Outputs Submitted For Award

Some papers are presented as preprint version and all my publications can be found in my Researchgate profile. https://www.researchgate.net/profile/Natasha_Ruiz

The book Apocalypse: The End of Antivirus are available at amazon.com and for free at:

https://www.researchgate.net/publication/280114888_Apocalypse_the_end_of_antivirus or https://www.Cyber_Security-review.com/wp-content/uploads/2017/02/APOCALYPSE-THE-END-OF-ANTIVIRUS.pdf

The outputs are presented in the same order listed in Table 1 excluded the book.

Tornando Pública a Navegação “In Private”

Rodrigo de S. Ruiz ¹, Fernando Pompeo Amatte ², Kil Jin Brandini Park D. Sc. ³

1, 2 Divisão de Segurança de Sistemas da Informação (DSSI)

Centro de Tecnologia da Informação Renato Archer (CTI)

Campinas – SP, Brasil.

3 Faculdade de Computação (FACOM) – Universidade Federal de Uberlândia

Monte Carmelo – MG, Brasil

rodrigo.ruiz@dssi.cti.gov.br, famate@gmail.com, kil@facom.ufu.br

Resumo — A crescente preocupação dos usuários com o sigilo dos dados gerados pelas atividades desenvolvidas no decorrer da navegação pelas páginas web fomentou o desenvolvimento de opções de navegação que ofertassem maior grau de segurança e sigilo para estes dados.

Se por um lado tal recurso, em caso de funcionamento perfeitamente alinhado as diretrizes de segurança, fornece ao usuário privacidade em suas atividades online, por outro lado fica claro que em caso de ilícitos cometidos, os agentes da lei têm que lidar com mais esta dificuldade para obter dados que forneçam provas necessárias durante uma investigação.

Independente do caso é importante verificar se as diferentes ofertas de mecanismo de navegação privada realmente funcionam.

A metodologia proposta mostrou que, dependendo do navegador utilizado, é possível recuperar dados em formato de texto sobre páginas visitadas durante a navegação sigilosa e até mesmo figuras que constituem essa página, em clara violação ao requisito funcional básico deste recurso.

Palavras-chave: Navegação sigilosa, Segurança de navegadores, Análise forense em navegadores.

Abstract — The growing concern of users about the confidentiality of data generated by web browsing activities made browser developers include options for safer and confidential browsing in their products.

For users those options, when functionally compliant with data security guidelines, guarantee online privacy. For law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering.

It is important to assess and validate private browsing techniques no matter which case.

The presented methodology shows that for some browsers it is possible to recover text and graphical data related to pages visited during private navigation, in clear violation of this tool basic functional requirement.

Keywords: Private browsing, Browser safety, Browser forensics.

I. INTRODUÇÃO

A crescente preocupação dos usuários com o sigilo dos dados gerados pelas atividades desenvolvidas no decorrer da navegação pelas páginas web fomentou o desenvolvimento de opções de navegação que ofertassem maior grau de segurança e sigilo destes dados.

A promessa dos desenvolvedores em relação ao funcionamento desse recurso é impedir que outros consigam reconstruir os passos que o usuário tomou durante suas atividades online.

Se por um lado tal recurso, em caso de funcionamento perfeitamente alinhado as diretrizes de segurança, fornece ao usuário privacidade em suas atividades online, por outro lado fica claro que em caso de ilícitos cometidos, os agentes da lei têm que lidar com mais esta dificuldade para obter dados que forneçam provas necessárias durante uma investigação.

Em ambos os casos, é importante verificar a funcionalidade real de tal recurso, se as implementações disponíveis realmente oferecem o sigilo ofertado, ou se existem falhas que possibilitem a obtenção de dados das atividades online mesmo com esta opção em uso.

Assim, o presente trabalho se estrutura nos seguintes tópicos:

Metodologia de Testes, onde se apresenta a metodologia aplicada aos testes efetuados da funcionalidade de navegação privada.

Resultados e Discussão, onde se apresenta os resultados obtidos pelos testes adotados e discute-se o tratamento apresentado para esses resultados.

Finalizando, seguem as conclusões e referências bibliográficas utilizadas.

II. METODOLOGIA DE TESTES

Ao testar uma funcionalidade de segurança, faz-se necessário definir os requisitos funcionais da mesma, além do perfil do atacante que tentará desabilitar ou sobrepujar tal funcionalidade.

Em um trabalho sobre análise da funcionalidade de navegação privada, [1] lista os perfis de possíveis atacantes, além dos modelos de segurança a serem verificados e os objetivos a serem cumpridos pelos navegadores que implementam a navegação privada.

No presente trabalho, parte-se do arcabouço metodológico apresentado por [1], para a construção do seguinte modelo metodológico:

O perfil do atacante considerado parte do pressuposto que este possui acesso local a máquina do usuário. Portanto, as tentativas de burlar o sistema de navegação privada ocorrerão a partir de uma imagem extraída da máquina do usuário.

Como o foco é avaliar a funcionalidade de navegação privada de modo isolado, considera-se que o usuário não adota técnicas de segurança que potencialmente influenciariam no acesso aos dados gerados durante a navegação. Assim, considera-se a não utilização de métodos criptográficos no disco da máquina do usuário.

Além disso, o presente trabalho foca a prospecção de dados na máquina do usuário em formato de texto ou figuras que tragam informações a respeito de páginas visitadas por este. Portanto, não é efetuada análise específica de alterações em arquivos utilizados por navegadores tais como histórico, cookies, cache, certificados e outros, cuja análise pode ser observada em [1] e [2].

Para os testes efetuados, criou-se uma máquina virtual “guest” padrão, com a instalação do sistema operacional Windows XP SP3 sobre uma máquina “host” executando o sistema operacional Ubuntu 10.04 e o virtualizador VirtualBox [3].

Um “snapshot” da máquina Windows recém instalada foi criado, considerando a possível necessidade de comparação futura da máquina base com as máquinas que executam os diferentes navegadores instalados.

Os navegadores testados foram o Internet Explorer 8 e o Firefox 8.0.1. Após cada teste, a máquina virtual Windows é levada ao seu estado inicial, imediatamente após a instalação do navegador em questão. Dessa forma, garante-se que todos os testes são efetuados sobre a mesma base.

Com base nestas premissas, efetuaram-se quatro testes diferentes para cada um dos navegadores em modo de navegação privada:

Teste 1: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Finalizar corretamente o navegador, gerar a imagem da máquina virtual para análise.

Teste 2: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Com o navegador ainda ativo, gerar a imagem da máquina virtual para análise.

Teste 3: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Requisitar que o sistema operacional interrompa o navegador, gerar a imagem da máquina virtual para análise.

Teste 4: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Requisitar que o virtualizador desligue a máquina virtual, simulando uma queda de energia, gerar a imagem da máquina virtual para análise.

Entende-se por imagem da máquina virtual, os arquivos separados de memória e disco da mesma.

Para cada teste efetuado, a imagem da máquina virtual gerada será analisada através da aplicação do programa strings [4] encontrado nas distribuições Linux, para a prospecção de cadeias de caracteres que tenham relação com a página web visitada.

Além disso, a imagem da máquina virtual também será analisada para a prospecção de arquivos gráficos associados à página visitada, através da utilização do programa scalpel [5], uma reconhecida ferramenta forense para extração de arquivos (“data carving”) de diferentes formatos.

Esta ferramenta funciona da seguinte forma: Ela lê um bloco de dados - memória, disco ou arquivos - e procura por assinaturas relacionadas a arquivos de formatos conhecidos.

Como essas assinaturas são uma sequência de bytes, existe a chance de ocorrência de falso-positivos e, portanto, a não captura do arquivo correto.

Além disso, é importante salientar a existência de diversos problemas conhecidos relacionados ao uso de ferramentas de “data carving”, como, por exemplo, suas limitações para o tratamento de dados não contíguos. Assim, é possível que uma imagem cuja sequência de bytes esteja dispersa não seja recuperada integralmente, apesar de sua possível existência no bloco de dados analisado.

III. RESULTADOS E DISCUSSÃO

Visando simular uma visita real a um site qualquer disponível na internet, uma seleção aleatória foi realizada, e o site escolhido para o experimento foi o [6]. Dado que algumas informações do site são proprietárias, as figuras recuperadas durante o teste, mesmo aquelas que foram completamente recuperadas serão reproduzidas apenas parcialmente no presente trabalho. O status de recuperação (parcial / total) será indicado na legenda associada à figura.

Para o navegador Internet Explorer 8, parte dos resultados obtidos foram:

A. Teste 1

1) Strings

```
<title>Simpsons.com.br </title>
<link rel="stylesheet" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style.css" type="text/css" media="screen" />
<link rel="alternate" type="application/rss+xml" title="Simpsons.com.br RSS Feed" href="http://www.simpsons.com.br/?feed=rss2" />
<link rel="pingback" href="http://www.simpsons.com.br/xmlrpc.php" />
<link rel="stylesheet" type="text/css" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style.css" />
<link rel="stylesheet" type="text/css" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style_ie.css" />
```

```
<link rel="stylesheet" type="text/css" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style_ie6.css" />
```

```
<link rel="stylesheet" href="http://www.simpsons.com.br/wp-content/plugins/share-buttons/css/share-buttons-user.css" type="text/css" />
```

```
seu voto:..http://thesimpsons.com/nedna/..." />
```

```
seu voto:..http://thesimpsons.com/nedna/..." />
```

```
<script type='text/javascript' src='http://www.simpsons.com.br/wp-includes/js/l10n.js?ver=20101110'></script>
```

```
<script type='text/javascript' src='http://www.simpsons.com.br/wp-content/plugins/share-buttons/js/share-buttons.js?ver=3.2.1'></script>
```

Theme Name: The Simpsons Theme

Description: The Simpsons Theme is a unique Widget ready WordPress theme with 2 columns, right sidebar and fixed width. Tested on Firefox, Internet Explorer 6, 7 and Opera.

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações a respeito da página visitada. Ao analisar o conteúdo completo gerado pelo programa strings, percebe-se que existe a possibilidade de reconstrução uma fração considerável da página visitada apenas com esses dados.

2) Figuras

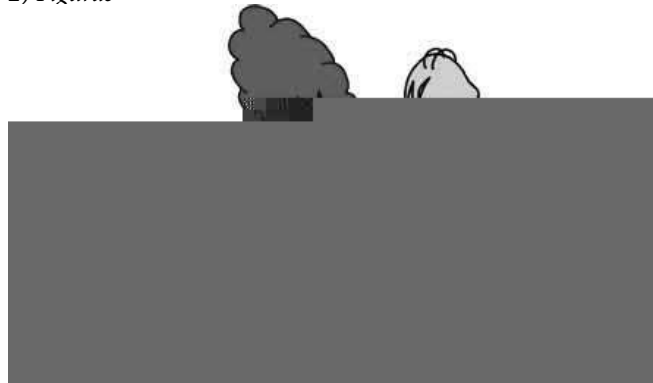


Figura 1 – Figura Parcialmente Recuperada do Sistema pelo Scalpel

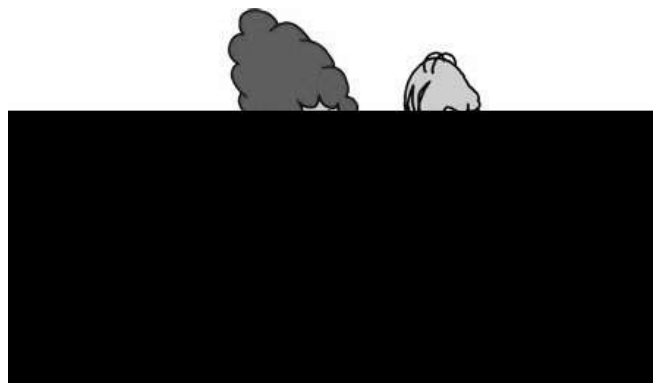


Figura 2 – Parte da Figura Original Encontrada na Página Visitada



Figura 3 – Parte da Figura Totalmente recuperada do Sistema pelo Scalpel

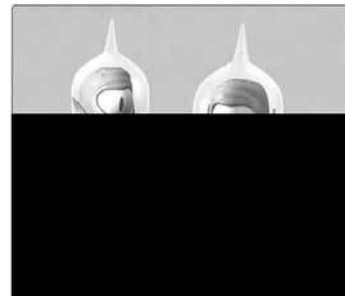


Figura 4 – Parte da Figura Original Encontrada na Página Visitada

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo recuperação de algumas delas.

B. Teste 2

3) Strings

Simpsons.jpg HTTP/1.1

simpsons`

ww.simpsonsE

www.simpsonsF

simpsons@-

eferer: http://www.simpsons.com.

simpsons.com.br/

simpsons@-

simpsons.com.br/

simpsons@-

simpsonsF

erer: http://www.simpsons.com.br

www.simpsons.com.br

simpsons.#

.simpsons.com.br%2F&extra_2=

: www.simpsons.c

simpsons.com.br

_simpsons_th@
 http://www.simpsons.com.br
 simpsons@[
 _url="http://www.simpsons.com.br/?p=148">S@
 Os Simpsons
 simpsons.com.br
 simpsons@-
 http://www.simpsons.com.br/favic
 simpsons.#
 Simpsons
 Simpsons
 www.simpsonsI
 tp://thesimpsons.com/nedna/c
 sidades sobre os Simpsons' class
 w.simpsons.com.br%2F&extr
 Os Simpsons
 simpsons@-
 Os Simpsons
 simpsons@-
 simpsons@-

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

4) Figuras



Figura 5 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

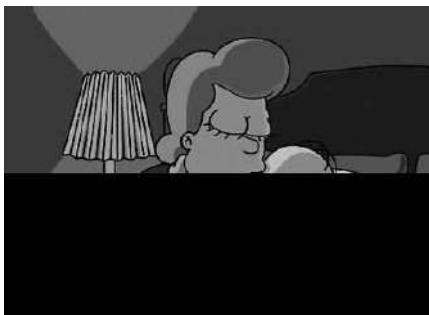


Figura 6 - Parte da Figura Original Encontrada na Página Visitada



Figura 7 - Parte da Figura Totalmente recuperada do Sistema pelo Scalpel



Figura 8 - Parte da Figura Original Encontrada na Página Visitada

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

C. Teste 3

5) Strings

w.simpsonsDr
 ww.simpsonsE
 simpsons.&W
 simpsons
 simpsons@R
 simpsons@-
 www.simpsonsK
 www.simpsonsE
 p://www.simpsons.com.br/
 www.simpsonsF
 : http://www.simpsona
 Referer: http://www.simpson
 : http://www.simpsonsE
 Simpsons.jpg HTTP/1.1
 .simpsons.com.br%2F&extra_2=
 dades sobre os Simpsons.

simpsons.#
 sidades sobre os Simpsons' class
 w.simpsons.com.br%2F&extra_2
 www.simpsons.com.br
 src="http://thesimpsons.com/nedn
 www.simpsonsHu
 ia Simpsons tem 3 re (
 www.simpsons@(.br/?p=129
 Os Simpsons
 www.simpsons.com.br
 Simpsons
 Os Simpsons
 %2F%2Fwww.simpsons.com.br
 mporada dos Simpsons.
 re Steve Jobs e Homer Simpson
 www.simpsons.com.br
 www.simpsons.com.br
 www.simpsonsA
 simpsons
 http://www.simpsons.com.br/wp-co
 title>Simpsons.com.br </
 simpsons@-
 dios de "Os Simpsons
 simpsons@-
 de Homer Simpson e sua fam
 simpsons@-
 u Simpsons - Escolha.

Novamente, pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

6) Figuras

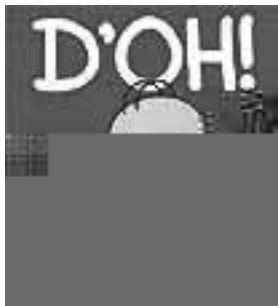


Figura 9 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

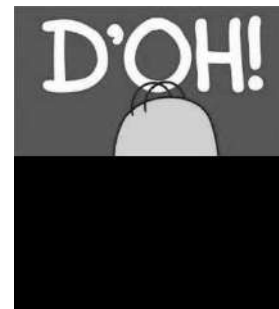


Figura 10 - Parte da Figura Original Encontrada na Página Visitada



Figura 11 - Parte da Figura Totalmente recuperada do Sistema pelo Scalpel



Figura 12 - Parte da Figura Original Encontrada na Página Visitada

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

D. Teste 4

7) Strings

Theme Name: The Simpsons Theme

Description: The Simpsons Theme is a unique Widget ready WordPress theme with 2 columns, right sidebar and fixed width. Tested on Firefox, Internet Explorer 6, 7 and Opera. Theme is XHTML/CSS valid and SEO friendly.

curtiu Globo adapta "Os Simpsons" para hor

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

Para o navegador Firefox, alguns dos resultados obtidos foram:

E. Teste 1

9) Strings

Nenhum resultado relevante

10) Figuras

Nenhum resultado relevante

F. Teste 2

11) Strings

Simpsons.com.br
thesimpsons
www.simpsons.com.br
http://thesimpsons.com/nedna/
www.simpsons.c
www.simpsons.com.br/wp-(
thesimpson
www.simpsons.com
www.simpsons.com.br
www.simpsons.com.br/?feed=rss2
simpsons@-
http://www.simpsons.com.br/wp-co
simpsonsC,
http://thesimpsons.com/nedna/col
HTTP:http://www.simpsons.com.br/
HTTP:http://www.simpsons.com.br/
simpsons@-
http://www.simpsonsAX!Q
dio dos Simpsons demor
www.simpsons.com.br

simpsons@-

/www.simpsons.com.br/wp-content/

www.simpsons.com.br/wp-includ%

a tema dos Simpsons.

www.simpsonsF

www.simpsons.com.br

www.simpsons.com.br

www.simpsonsC

ost: thesimpsons.com

/03/RockBottomSimpsons.jpg

www.simpsonsD[

r: http://www.simpsons.com.br/

www.simpsonsA;

www.simpsons.com.br

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

12) Figuras



Figura 17 - Figura Parcialmente Recuperada do Sistema pelo Scalpel



Figura 18 - Parte da Figura Original Encontrada na Página Visitada

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação das mesmas.

G. Teste 3

13) Strings

www.simpsons.com.br

Referer: http://www.simpsona;
.simpsons.

www.simpsonsD'

Referer: http://www.simpsonsAY
thesimpsons.com

www.simpsons.com.br

Referer: http://www.simpsonsA;

simpsons@-

Referer: http://www.simpsonsA;

content/uploads/2010/03/simpsons

Host: www.simpsons.com.br

simpsonsA

simpsons@-

r: http://www.simpsons.com.br/

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

14) Figuras

Não foram recuperadas figuras relativas a página visitada.

H. Teste 4

15) Strings

Não foram recuperadas strings de texto referentes a página visitada.

16) Figuras

Não foram recuperadas figuras referentes a página visitada.

Agrupando os resultados obtidos, tem-se:

Tabela 1 – Resultados para o navegador Internet Explorer

	Teste 1	Teste 2	Teste 3	Teste 4
Recuperação de endereço da página visitada	Sim	Sim	Sim	Sim
Recuperação de figuras parciais	Sim	Sim	Sim	Sim
Recuperação de figuras completas	Sim	Sim	Sim	Sim

Tabela 2 – Resultados para o navegador Firefox

	Teste 1	Teste 2	Teste 3	Teste 4
Recuperação de endereço da página visitada	Não	Sim	Sim	Não
Recuperação de figuras parciais	Não	Sim	Não	Não
Recuperação de figuras completas	Não	Não	Não	Não

Pode-se verificar que a função de navegação privada, tal como implementada, apresenta-se funcionalmente mais adequada no navegador Firefox.

IV. CONCLUSÃO

Nos quatro tipos de testes realizados, é possível verificar que a versão testada do Internet Explorer possui sérias falhas em sua funcionalidade de navegação privada, ao deixar disponível no sistema uma série de informações que possibilitariam não apenas identificar páginas visitadas como também reconstruí-las.

Já o navegador Firefox apresenta dados relativos à página visitada apenas nas análises desenvolvidas tanto com o navegador executando (teste 2) quanto logo após o sistema ter interrompido sua execução (teste 3).

Assim, pode-se concluir que para a metodologia adotada, a funcionalidade de navegação privada implementada no Firefox mostra-se mais adequada que aquela encontrada no Internet Explorer.

Se por um lado isso representa um ponto negativo para o usuário, por outro facilita o trabalho de perícia dos navegadores por agentes da lei nos casos em que esta tarefa se faz necessária.

V. REFERÊNCIAS BIBLIOGRÁFICAS

- [1] AGGARVAL, G. BURSZEIN, E. JACKSON, C. BONEH, An Analysis of Private Browsing Modes in Modern Browsers. USENIX 2010, Disponível em: <http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf>. Acesso em: 30 jun 2012.
- [2] MAHENDRAKAR, A. IRVING, J. PATEL, S. Forensic Analysis of Private Browsing Mode in Popular Browsers. Disponível em: <http://mocktest.net/paper.pdf>. Acesso em: 30 jun 2012.
- [3] VirtualBox. Disponível em: <https://www.virtualbox.org/>. Acesso em: 30 jun 2012.
- [4] Strings manpage. Disponível me: <http://linux.die.net/man/1/strings>. Acesso em 30 jun 2012.
- [5] Scalpel. Disponível em: <http://www.digitalforensicsolutions.com/Scalpel/>. Acesso em 30 jun 2012.
- [6] Simpsons.com.br. Disponível em: <http://www.simpsons.com.br/>. Acesso em 30 jun 2012.

Rodrigo de Souza Ruiz é servidor do Centro de Tecnologia da Informação Renato Archer. "Agradeço ao empenho dos meus amigos Fernando e Kil que tornaram possível essa pesquisa e especialmente a minha mulher, Gilce Ganzert Ruiz, pela inspiração e apoio ao meu trabalho."

Fernando Pompeo Amatte, com mais de 20 anos de experiência na área de segurança da informação, possui as certificações profissionais CISSP, GCIH e MCSO. Com experiências em provedores de acesso, empresas multinacionais de telecomunicação e setor financeiro. Atua como consultor de segurança da informação e como professor nos cursos de Pós-Graduação da Veris Educacionais (IBTA) e SENAC em Campinas. Pesquisador de malwares, é também perito de informática para o Tribunal Regional do Trabalho de Campinas.

Kil Jin Brandini Park, D. Sc., é especialista em segurança da informação, engenheiro de computação pela UNICAMP e doutor pela mesma instituição. Atua como professor adjunto da faculdade de computação - FACOM, da universidade federal de Uberlândia - UFU, Campus Monte Carmelo.

Opening the “Private Browsing” Data – Acquiring Evidence of Browsing Activities

Rodrigo de S. Ruiz ¹, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc. ³

1 Malware Analysis Nucleus (NUCAM)

Renato Archer Information Technology Center(CTI)
Campinas – SP, Brazil.

2 Independent Researcher, Campinas – SP, Brazil.

3 Computer Faculty (FACOM) –Federal University of Uberlândia
Monte Carmelo – MG, Brazil

rodrigossruiz@outlook.com, famate@gmail.com, kil@facom.ufu.br

Abstract — The growing concern of users about the confidentiality of data generated by web browsing activities made browser developers include options for safer and confidential browsing in their products.

For users those options, when functionally compliant with data security guidelines, guarantee online privacy. For law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering.

No matter which case, it is important to assess and validate private browsing techniques.

The presented method shows that for some browsers it is possible to recover text and graphical data related to pages visited during private navigation, in clear violation of this tool basic functional requirement.

Keywords: Private browsing, Browser safety, Browser forensics.

1 INTRODUCTION

The growing concern of users with the confidentiality of the data generated by the activities developed in the course of navigation through web pages fostered the development of navigation options that offer greater degree of security and confidentiality of the data.

The promise of the developers regarding the operation of this feature is to prevent others to reconstruct the steps the user took during his online activities.

On Mozilla’s page we found this commercial text about privacy and private browsing:

“Sometimes it’s nice to go undercover: Open a private window and protect your browsing history. You can switch between private and normal windows quickly, so it’s easy to go back to what you were doing before. This feature is great if you’re doing your online banking on a shared computer or checking email from an Internet café.”
[1]

On Chrome’s browser, when the user enable incognito mode, the new tab opened displays the following message:

*“You came in incognito mode. Pages you view in this window will not appear in your browser history or search history will **not leave other traces**, like cookies, on your computer after you close all incognito windows open. However, all the downloads you make or bookmarks you create will be preserved.”*

On Safari’s page we found this commercial text about privacy and private browsing:

“...Safari can keep your browsing history private. When you turn on Private Browsing, Safari does not remember the pages you visited, your search history, or your AutoFill information...”[2]

On IE’s page we found this commercial text about privacy and private browsing:

“While you are surfing the web using InPrivate Browsing, Internet Explorer stores some information—such as cookies and temporary Internet files—so the webpages you visit will work correctly. However, at the end of your InPrivate Browsing session, this information is discarded...”[3]

On the one hand such a feature, if operating perfectly aligned with security guidelines, provides the user privacy in their online activities, on the other hand it is clear that in case of unlawful behavior, law enforcement officers have to deal with this layer of protection to obtain the necessary data to provide evidence during the course of an investigation.

In both cases, it is important to verify the actual functionality of such a feature, if available implementations actually provide the degree of confidentiality offered, or if there are flaws that allow the retrieval of online activity data.

This paper is an extended version of a work previously presented by the authors [4], with additional results and analysis, and is structured in the following topics:

Method and Tests, which presents the method applied to tests performed in various browsers with the private browsing feature enabled.

Results and Discussion, which presents the results obtained by the tests adopted and discusses these results.

Finally, follow the conclusions, further studies and references used.

2 METHOD AND TESTS

When testing a security feature, it is necessary to define its functional requirements and the profile of the attacker who will try to disable or override this feature.

In a paper on the analysis of private browsing functionality, [5] lists the profiles of potential attackers, security models to be checked and the objectives to be met by browsers that implement private browsing. In this work, we start from the methodological framework presented by [5], for the construction of the following methodological model:

The profile of the attacker considered assumes that he has local access to the user machine. Consequently, attempts to circumvent the system of private browsing will occur from an image taken from the user's machine hard drive.

As the focus of the evaluation is the private browsing feature, we considered that the user does not adopt other security tools or techniques that could exert influence on the access of the data generated during navigation. Thus, we did not conduct any test with the adoption of cryptographic methods in the disk of the user's machine.

Furthermore, this paper focus on searching the user's machine for fragments of data from which text or images that brings information about pages visited could be extracted. Therefore, the specific analysis of changes to files used by browsers such as history, cookies, cache and certificates was not performed. Such analysis can be found in [5] and [6].

We tested Internet Explorer browser on bare metal hardware with the use of four notebooks equipped with Windows 7 Pro SP1.

For the other tests performed, we created a standard guest virtual machine - with the operating system Windows 7 Pro - in the host operating system - Windows 7 Pro - using the virtualization software Virtual Box [7].

An export (snapshot) of the newly installed Windows machine was created, considering the possible need for future comparison of the base guest machine with guest machines running the different browsers tested.

The browsers tested were Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1 and Safari 5.1.7_1. The base guest virtual machine for each browser was replicated 4 times, each to be used in the four different tests performed on each browser.

Based on those configurations, four different tests for each browser in private browsing mode were applied:

Test S (Shutdown): Consists of visiting a web site available on the internet, making operations to interact with the site, finish the execution of the browser correctly and generating the virtual machine image for analysis.

Test F (Freeze): Consists of visiting a web site available on the Internet, making operations to interact with the site and with the browser still active, generating the virtual machine image for analysis.

Test K (Kill process): Consists of visiting a web site available on the internet, making operations to interact with the site, requesting that the operating system interrupt the browser execution and generating the virtual machine image for analysis.

Test P (Power down): Consists of visiting a web site available on the internet, making operations to interact with the site, requesting the virtualizer to turn off the virtual machine - simulating a power outage - generating the virtual machine image for analysis.

For each test performed, the virtual machine image generated will be analyzed through the application of the program strings [8] found in many different Linux distributions.

This program is used for the search of strings inside the virtual machine images that could present relation to the webpage visited.

The images of the virtual machines will be analyzed for the search of graphic files associated with the visited webpage, through the usage of the foremost program [9], a renowned forensic tool for extraction of files - "data carving" - of different formats.

This tool works as follows: It reads a block of data - memory, disk or files - and looks for signatures related to files of well-known formats. It is noteworthy that in the present research we investigated only the persistent memory (i.e. physical and virtual disk).

Since these signatures are a sequence of bytes, there is the chance of occurrence of false positives and therefore the capture of incorrect file.

Furthermore, it is important to note that there exist several known problems associated with the use of tools aiming for "data carving", for example, limitations to the treatment of non-contiguous data. Thus, it is possible that an image whose sequence of bytes is dispersed will not be fully recovered, despite its possible existence in the block of data analyzed.

The WinHex tool was also used to search for keywords found in the navigated webpage.

3 RESULTS

Aiming to simulate an actual visit to any website available on the internet, a random

selection was made, and the site chosen for the experiment was the [10]. Since some site information is proprietary, the figures recovered during the test will be only partially reproduced in the present work. We would like to acknowledge that those information are copyright of their respective owners.

SAFARI Browser

For the Safari browser, the following results were obtained:

F test (freeze)

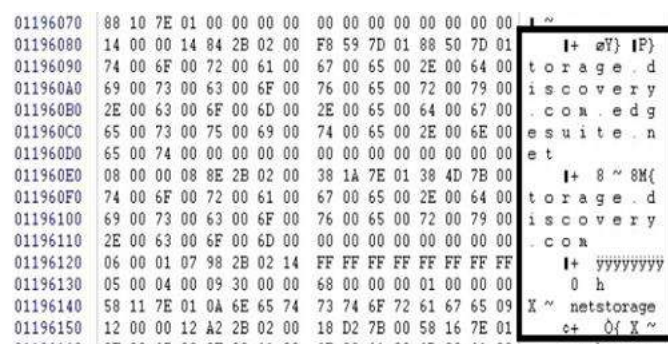


Figure 1- "storage.discovery.com" string located in virtual machine's image.

No image fragments were found on the virtual machine's hard disk image.

K Test (kill process)

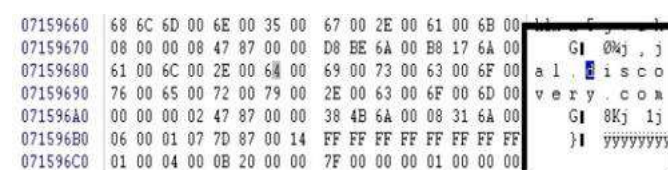


Figure 2- "discovery.com" string located in virtual machine's image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 3 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

p://dsc.discovery.com/videos

<http://store.discovery.com/?ecid=PRF-DSC-101345&pa=PRF-DSC-101345>

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 4 –Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

<http://store.discovery.com/discovery/layout/favicon.ico>
<http://dsc.discovery.com/>
<http://games.dsc.discovery.com/>
<http://dsc.discovery.com/tv-shows>
<http://store.discovery.com/discovery/layout/favicon.ico>

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 5 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

<http://dsc.discovery.com/tv-shows>
<http://dsc.discovery.com/>
<http://store.discovery.com/discovery/layout/favicon.ico>
<http://dsc.discovery.com/videos>
america.discovery.com.edgesuite.net
velocity.discovery.com
metrics.discovery.com
orate.discovery.com
animal.discovery.com.edgesuite.net

The results obtained for the Safari browser tests are grouped in table 1:

Table 1 – Results for Safari Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

FIREFOX browser:

F Test (freeze)

```
0F 00 00 A0 00 00 01 21 3F 20 02 E2 00 7F 00 70 17 a p
A2 7F 1F 73 63 2E 64 69 73 63 6F 76 65 72 79 2E c sc. Discovery.
63 6F 6D 2F 76 69 64 65 6F 2D 74 6F 70 69 63 73 com/video-topics
2F 61 64 07 76 65 6E 74 75 72 65 00 42 7F 03 1A /ad venture B
F0 3E 6D 40 7F 00 D0 E0 0B 7F 20 6B 02 58 6F EA >m@ Dà k Xoë
60 7F 00 F0 A0 7F 00 80 20 13 A0 7E E0 01 7F 03
```

Figure 6 –“sc.discovery.com/video-topics” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test (kill process)

```
74 69 6D 69 7A 65 6C 79 42 75 63 6B 65 74 73 2E timizelyBuckets.
64 69 73 63 6F 76 65 72 79 2E 63 6F 6D 2F 7D 2A discovery.com/*
09 07 33 29 0F 08 08 01 6F 70 74 A0 28 08 45 6E 3) opt ( En
64 55 73 65 72 49 64 E0 06 2A 03 09 29 07 31 E0 dUserIdà * ) là
06 2A 05 53 65 67 6D 65 6E E0 08 54 04 7C 1B 07 * Segmenà T |
10 2F 10 FA 10 EF EF 2F 7A 6D 7A 2F 6D 6F 7A 60
```

Figure 7 – “discovery.com” string located in the virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 8 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:


```

66 75 6C 6C 79 51 75 61 6C 69 66 69 65 64 55 52 fullyqualified
4C 3A 22 68 74 74 70 3A 2F 2F 64 73 63 1F 2E 84 L:"http://dsc.d
69 73 63 6F 76 65 72 79 2E 63 6F 6D 2F 74 76 2D iscovery.com/tv-
73 68 6F 77 73 2F 73 75 72 76 69 75 6F 72 03 6D shows/survivor h
61 6E 2F 60 5E 0B 73 2F 62 75 72 6E 2D 62 61 62 an/^ s/burn-bab
79 2D 40 09 11 2E 68 74 6D 22 2C 64 75 72 61 74 y-@ .hta",durat
    
```

Figure 13 – “discovery.com/tv-shows” string located in the virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

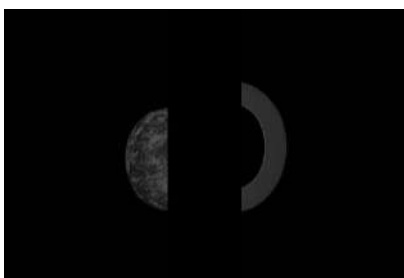


Figure 14 – Image recovered on hard disk image analysis and found on Discovery.com website.



Figure 15 – Image recovered on hard disk image analysis and found on Discovery.com website.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

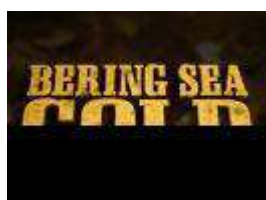


Figure 16 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

```

//dsc.discovery.com/
://static.ak.facebook.com/connect/xd_arbiter.php?vers
ion=27#cb=fdde13148&domain=dsc.discovery.com&ori
gin=http%3A%2F%2Fdsc.discovery.com%2F2a7e0cd34
&relation=parent&error=unknown_user
/dsc.discovery.com/tv-shows
    
```

```

://dsc.discovery.com/
://dsc.discovery.com/
://dsc.discovery.com/
http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/
    
```

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 17 - Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

```

": "Survivorman Videos", "srcUrl": "", "uuid": "8e18dcd9-
8d1d-11e2-a7b7-06a90ff35868", "bdat": "must
watch", "keywords": "survivorman, 10 days, ten, days, must
watch, mexico, tiburon, deserted, island, les
stroud, survival, survivor, man, water, pool, algae, fresh, cane
, reed, sludge", "mediaType": "lift", "mp4": [{"bitrate": "110
k", "src": "http://discsmil.edgesuite.net/digmed/hdnet/07/a
7/13776400801197_102MissingPiece-
110k.mp4"}], "akamaihd.net/i/digmed/hdnet/98/9a/137764
01201197_104Stove-
, 400k, 110k, 200k, 600k, 800k, 1500k, 3500k, .mp4, csmil/mast
er.m3u8", "networkId": "DSC", "thumbnailURL": "http://ne
tstorage.discovery.com/feeds/brightcove/asset-
thumbnails/dsc/0a5dbdfa893fec1f556a7d81c5b28bc470e
cbb0e_0a5dbdfa893fec1f556a7d81c5b28bc470ecbb0e.jp
g"
    
```

Table 3 – Results for Chrome Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

INTERNET EXPLORER Browser

F Test (freeze)

```

60 DE B2 0A 10 D5 7C 0A 35 00 33 00 41 00 25 00 2 5 3 A %
32 00 35 00 32 00 46 00 25 00 32 00 35 00 32 00 2 5 2 F % 2 5 2
46 00 64 00 73 00 63 00 2E 00 84 00 69 00 73 00 F d s c . i s
63 00 6F 00 76 00 65 00 72 00 79 00 2E 00 63 00 c o v e r y . c
6F 00 6D 00 25 00 32 00 35 00 32 00 46 00 66 00 o n % 2 5 2 F f
32 00 32 00 61 00 33 00 35 00 38 00 33 00 33 00 2 2 a 3 5 8 3 3
31 00 32 00 34 00 33 00 36 00 32 00 25 00 32 00 1 2 4 3 6 2 % 2
    
```

Figure 18 – “discovery.com” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test(kill process)

```

0C 00 01 01 87 00 04 01 B2 00 01 68 00 74 00 74 I 3 h t t
00 70 00 3A 00 2F 00 2F 00 73 00 74 00 6F 00 72 p : / / s t o r
00 65 00 2E 00 64 00 69 00 73 00 63 00 6F 00 76 e . d i s c o v
00 65 00 72 00 79 00 2E 00 63 00 6F 00 6D 00 2F e r y . c o m /
00 6A 00 73 00 2F 00 61 00 6A 00 61 00 78 00 2F j s / a j a x /
00 61 00 6A 00 61 00 78 00 44 00 65 00 74 00 61 a j a x D e t a
00 69 00 6C 00 2D 00 31 00 2E 00 32 00 2E 00 6A i l - 1 . 2 . j
00 73 00 3F 00 76 00 65 00 72 00 3D 00 31 00 30 s ? v e r = 1 0
    
```

Figure 19– “http://store.discovery.com/js/ajax/” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 20 – Image recovered on hard disk image analysis and found on Discovery.com website.

S Test (Shutdown)

On this test, another step taken was the analysis of log files generated by the Internet Explorer browser. It is easy to see that the page address is easily visible inside a log file:

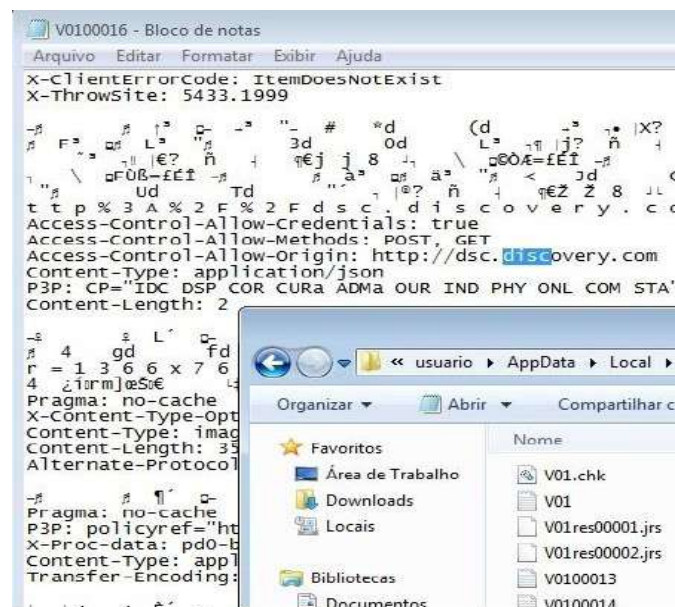


Figure 21 – Log file found using only the explorer and notepad. They demonstrate the system failure (string <http://dsc.discovery.com> found) in the private-IE10.

Table 4 – Results for IE10

	F Test	K Test	P Test	S Test
Page address recovery	Yes	Yes	No	Yes
Picture recovery	No	No	Yes	No

Further analysis to prospect the files and directories involved in the data leakage generated the following results:

In all browsers, some of the data associated with the navigation could be extracted from the file pagefile.sys. This proves that part of the data is leaking through the paging process’s storage mechanism used by the operating system.

In Internet Explorer’s case, more data could be found in a file located at the directory:

user\<username>\appdata\local\microsoft\windows\temporary internet files\low\content.ie5\ndm4l4gv\

On Chrome’s case, more data could be found in the file:

user\administrador\appdata\local\microsoft\windows\webcache\webcache\01.dat

Those files points to the fact that navigation data is leaking from cache files used by the browsers.

4 DISCUSSION

From the data generated by the tests, it is possible to assume that every implementation of the private browsing functionality in all browsers tested demonstrate some type of failure.

In some cases, those flaws allow an attacker to identify the pages visited by the user. In other cases, they generate enough data to allow the partial reconstruction of the pages visited.

We contact the developers about the results and obtained some mixed comments.

Microsoft answer to our request for comment:

*"...We do encourage security researchers we are working with to present their research at events...
...The issue is still being scoped and researched. I will let you know once that has finished and a servicing decision has been made"*

From the information about the private browsing functionality and the answers received, it is possible to extract that the average user is not well informed of the limitations inherent to the implementations of the service.

5 CONCLUSION

In all four types of tests performed, it is possible to verify that all browsers tested presented flaws in their private browsing feature.

Those flaws generates data that remains available in the system and allow not only the identification of pages visited but in some cases also to partially rebuild them.

Browsers promises to leave no traces of the navigation activities of users. This work proves that privacy as advertised is not provided.

In face of the results obtained, we would like to recommend the developers to explicitly alert the users about the limitations of the private browsing functionality implementation.

We would like to praise Microsoft's answer because they both acknowledged the information received and approved the release of the study.

If on one hand this is a negative point for the user, on the other hand those flaws facilitate the work of law enforcers in cases where there is need for the data related to the navigation activity.

6 FURTHER STUDIES

In future researches, we plan to analyze the mechanisms and data structures - both browser and operating system related - involved in the browsing activities data leakage in-depth. This line of study could bring forth new techniques to avoid the problems presented in this paper on the implementations of the private browsing functions.

7 REFERENCES

- [1] Mozilla private browsing. Available at: <http://www.mozilla.org/en-US/firefox/features/> Accessed at: Oct, 24, 2013
- [2] Archived - Mac Basics: Safari 5.1. Available at: <http://support.apple.com/kb/ht4550>. Accessed at: Nov, 21, 2013.
- [3] What is InPrivate Browsing? Available at: <http://windows.microsoft.com/en-us/windows7/what-is-inprivate-browsing>. Accessed at: Nov, 21, 2013.
- [4] RUIZ, R. S., AMATTE, F. P., PARK, K. J. B. Tornando Pública a Navegação "InPrivate". Proceedings of the IcoFCS2012. Available at: http://www.icofcs.org/2012/ICoFCS2012_Full.pdf. Accessed at: Nov, 21, 2013.
- [5] AGGARVAL, G. BURSZEIN, E. JACKSON, C. BONEH, An Analysis of Private Browsing Modes in Modern Browsers. USENIX 2010, Available at: <http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf>. Accessed at: Jun, 30, 2012.
- [6] MAHENDRAKAR, A. IRVING, J. PATEL, S. Forensic Analysis of Private Browsing Mode in Popular Browsers. Available at: <http://mocktest.net/paper.pdf>. Accessed at: Jun, 30, 2012.
- [7] VirtualBox tool. Available at: <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>. Accessed at: Jun, 13, 2013.
- [8] Strings man page. Available at: <http://linux.die.net/man/1/strings>. Accessed at Jun, 30 2012.
- [9] Foremost website. Available at: <http://foremost.sourceforge.net/> Access at: Oct 14, 2012.
- [10] Discovery.com website. Available at: <http://dsc.discovery.com>. Accessed at: Oct, 07, 2012.

Security Issue on Cloned TrueCrypt Containers and Backup Headers

Rodrigo de S. Ruiz ¹, Fernando Pompeo Amatte ², Kil Jin Brandini Park D. Sc. ³

1, 2 Núcleo de Coleta e Análise de Malware (NUCAM)

Renato Archer – Information Technology Center (CTI)

Campinas – SP, Brasil.

3 Computer Faculty (FACOM) –Federal University of Uberlândia

Monte Carmelo – MG, Brazil

rodrigoruiz@hotmail.com, famate@gmail.com, kil@facom.ufu.br, <http://www.cti.gov.br/nucam/>

ABSTRACT

The growing concern of various entities with the confidentiality of the data ultimately fostered the development of tools for data protection at various levels, from a simple password protection on a word processor to sophisticated methods of encryption based on hardware or software implementation.

On the one hand such a feature, if operating perfectly aligned to security guidelines, provides the user privacy in its activities, on the other hand it is clear that in case of unlawful behavior, for law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering.

This study aims to present a different and little explored approach to access information inside containers encrypted through the usage of Truecrypt software.

The proposed methodology proved that, in certain circumstances, a Truecrypt container presents a technical and operational vulnerability ignored by business and IT professionals, in clear violation of the basic functional requirement of this feature.

KEYWORDS

Encryption, Confidentiality, Data security, forensics, Truecrypt.

1 INTRODUCTION

The growing concern of various entities with the confidentiality of the data ultimately fostered the development of tools for data protection at various levels, from a simple password protection on a word

processor to sophisticated methods of encryption based on hardware or software implementation.

This study aims to present a different and little explored approach to break containers encrypted through the usage of Truecrypt software.

The promise of the developers regarding the operation of this feature is to prevent unauthorized access on information recorded in a Truecrypt container.

On the one hand such a feature, if operating perfectly aligned to security guidelines, provides the user privacy in its activities, on the other hand it is clear that in case of unlawful behavior, for law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering during an investigation.

The Truecrypt is a multi-platform cryptographic tool very popular among IT professionals and consequently largely adopted in various governmental and business ventures.

Depending of the circumstances, data protection is equivalent to protecting assets, reputation and in some cases even philosophical and physical freedom.

In this context, the assessment of functional correctness of the tool is of paramount importance.

Thus, this paper is structured in the following topics:

Related work, where other researches and methodological treatment related to these paper topics are discussed.

Presentation of Truecrypt, where the software features are described as provided by its developers.

Presentation of the vulnerable user profile, which describes the characteristics of potentially vulnerable users.

Testing Methodology, which presents the methodology of tests applied in order to acquire sensitive information.

Results and discussion, which presents the results obtained by the tests adopted and discusses the treatment presented for those results.

Finally, follow the conclusions and references used.

2 RELATED WORK

On the discussion of Block Ciphers, [1] classifies the possible attacks attempts based on the data that an attacker can procure:

- Ciphertext-only attack, where an attacker has access only to ciphered information.
- Know plaintext attack, where an attacker has access to plaintext messages and its ciphered counterparts.
- Chosen plaintext attack: where the attacker chooses a specific set of plaintext messages and is able to acquire its ciphered counterparts.
- Adaptively chosen plaintext attack: where an attacker chooses the plaintext messages based on the cipher result of the previous chosen plaintext message.
- Chosen ciphertext attacks: where an attacker chooses different ciphered messages and is able to acquire its deciphered counterparts.

Furthermore, [2] divides possible attacks in two categories:

- Practical attacks, that focus on implementation and usage issues.
- Theoretical attacks, that focus on the mathematical aspects of the chosen cipher algorithms.

Proposing a methodology to evaluate a given system security, [3] presents the attack tree, a structure that describes a system security using different attack possibilities as parameters. It also gives an example attack tree on the PGP e-mail security software:

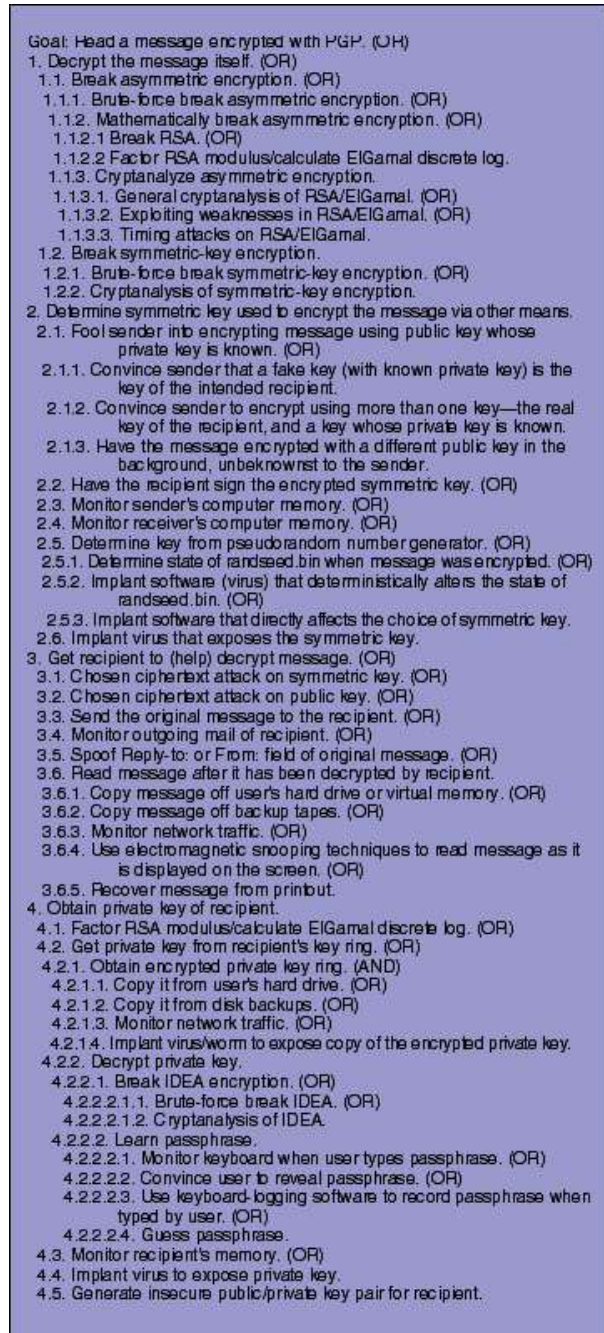


Figure 1 - Attack Tree Against PGP. Source: [3] SCHNEIER, 1999.

As the author pointed, the previous attack tree can easily be extended to include more attack formats.

Although the tree is based on PGP, it could easily fit the TrueCrypt software. Besides that, on the previous example, one possible inclusion under item 1 of the tree could be item 1.3 –

“Exploit software implementation weakness”. This kind of attack would, through the active exploitation of the software design issues or vulnerabilities, lead to full message decryption. Under [1] and [2] classification system, proposed attack 1.3 would be a ciphertext-only and practical instead of theoretical. This paper methodology is based on this attack type.

3 PRESENTATION OF TRUECRYPT

For the presentation, we took the liberty of reproducing some words from the developers:

“TrueCrypt is software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. Entire file system is encrypted (e.g. file names, folder names, contents of every file, free space, meta data, etc).”[4]

Recognized worldwide and with much acceptance among IT professionals, this free software is used both by individuals and by various governmental and business ventures concerned with the confidentiality of their data.

The Federal Police of Brazil in partnership with the FBI tried for more than one year to break the cryptographic code files generated by Truecrypt and seized in an investigation of bank fraud with international repercussions. The National Institute of Criminology (INC) using the most advanced techniques could not decode the passwords of those files. The Brazilian government also announced that there are no legal instruments that could be used to force developers to reverse the code and give free access to the information.[5]

This famous legal case with high visibility was presented by the software developers as a proof of the software importance, with the message that neither the Brazilian Federal Police nor the FBI managed to break the security of Truecrypt.

4 VULNERABLE USER PROFILE

It is a known fact that the choice of professionals who provide technical support to a large portion of politicians, businessmen and professionals from various sectors is done by concepts that exclude technical competence, which is replaced by degree of confidence. In extreme cases, this leads to recruitment of unprepared employers, unable to provide the correct solutions to technological problems.

Such behavior has the potential to create security holes that can be exploited by both criminals and the police.

Together with technical ineptitude, unlawful and unethical behavior are also causes of data security breaches.

A large Brazilian oil company reported that the theft of equipment containing sensitive information about the discovery of new oil wells affected the value of its shares negotiated on the stock market. [6]

A survey by the Ponemon Institute presents interesting and alarming data on the damage caused to businesses, where the theft of a laptop can cost up to \$ 115,000 in strategic information loss.

The same survey shows that the encryption significantly reduces the cost of the theft: while the theft of a machine with unencrypted HD costs U.S. \$ 56,165, one that was encrypted presents the loss of U.S. \$ 37,443 [7]

The risk of infiltration by criminal elements in business and in their own governments makes the population vulnerable to manipulation and loss of confidential data.

Both businesses and governments are subject to such infiltration. Criminal organizations are allocating their representatives in strategic positions for the purpose of illicitly obtaining precious inside information. Criminals go so far as to sponsor people in their studies to fulfill this goal. [8] [9].

A report in ComputerWorld magazine's website has attracted attention by bringing up actual cases of IT professionals very well placed in large and reputable companies, using their positions of trust to commit crimes. This report also presents research, which suggests that one in three IT professionals spy systems of the company and his colleagues, accessing data such as contracts, wages, emails, and other strategic information. [10]

5 METHODOLOGY FOR TESTING

When testing a security feature, it is necessary to define the functional requirements of the same, and the profile of the attacker that will try to disable or override this feature.

In this work, we start from the methodological framework presented by [11] for the construction of the following methodological model:

The profile of the attacker assumes that it has access to the user's Truecrypt container at two different times. When it was first created and after the user stored valuable information on it and changed its password.

As the focus is to evaluate the functionality of password protection of a Truecrypt container, other aspects such as the type of encryption used and the use of full protection of the disk will not be addressed in this work.

Furthermore, this paper focuses on extracting data in the container used to access the user confidential information without access to the password of the container and without the use of a password cracking software (pure brute force or dictionary attack).

For the tests performed, we used the following tools and software. A notebook equipped with Intel © Pentium © Dual Core with 3.0 GB of memory.

Truecrypt 7.1 software released on feb/07/2012 downloaded from <http://www.truecrypt.org/downloads> on 20/04/2013 and PERL programming language.

The tests were conducted as follows:

With Truecrypt installed, we created a container with size of 292KB, AES encryption with SHA-512 hash algorithm.



Figure 2 - Creation of container.

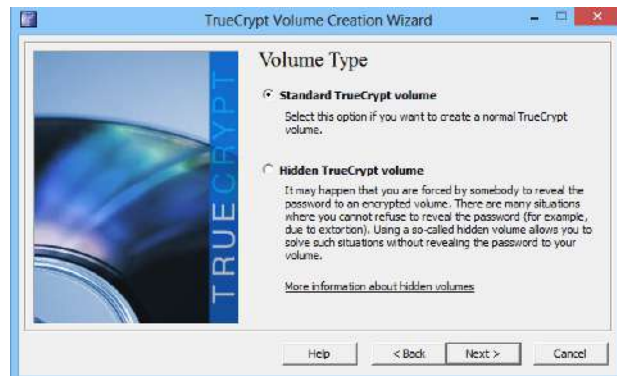


Figure 3 - Creation of container



Figure 4 – Choosing file name.



Figure 5 – Choosing encryption schemes



Figure 6 - Selecting the file size.



Figure 7 – Choosing password. The container was created with password equal to 123.



Figure 8 - Formatting container.

This container was sent to several people with different profiles, entrepreneurs, researchers, politicians and other professionals with the following text:

“Dear Sir,

We ask you kindly to participate anonymously in a survey about the security offered by the data encryption program Truecrypt.

If you accept it, we guarantee the confidentiality of your participation and ask that you open the attached file in your Truencrypt program; the password for access is 123.

Record in this container some information that only you know and change the password of the container to a complex password of your choosing and resubmit the container for us.

By agreeing to participate in the research you agree with our attempt to locate and access the information added to the container.”

We limited to this research to the first 6 valid received files.

The following procedure was applied to the received containers:

To validate the files, we attempted to access the container using the default password 123. In cases where this password was accepted, the file was immediately discarded.

If the password 123 was rejected the file went to the sample set.

The files received and included in the sample set are listed below.

Table 1 - Files validated and stored in the sample set

Files	Data file
cae6a29442b290f3f9f2b668d955435a	D1
b2c1b4a0a5c07edfe94143283f98968d	D2
7fb2155000da28c4967043e46559e168	D3
a6f94e886dba0e39234ed1a7f034b0f5	D4
5d8d383377906bd0390e79cdef5b55c5	D5
b3ff511739ee282528a960695352ee77	D6
4af8e8b12093c4ca8da0ae9fbf9ed8eb	D0

Note the addition of the file identified as D0, which is the original empty file sent to all participants.

6 RESULTS AND DISCUSSION

The hypothesis to be tested emerged from the analysis of the hex code of a file created by Truecrypt and the comparison of the hex code of the

same file after executing the procedure to change the user's password to access the container.

Since this preliminary analysis showed that the container did not change, unlike the header, which presented obvious changes, the possibility of manipulating the Truecrypt file to access the container without access to the current user's password in case of possession of one previous valid header with known password was tested.

To assess this, the original header was saved and later merged to the TrueCrypt container after it went through the password change.

To manipulate the files we applied the following code written in Perl.

```
# Fernando Pompeo Amatte
# 07/abr/2013
#! /usr/bin/perl
file1 = $ ARGV [0];
$ file2 = $ ARGV [1];
$ source = $ ARGV [2];
$ size = $ ARGV [3];
open (FILE, "$ file1");
binmode FILE;
open (QRA, "> $ file2");
binmode QRA;
seek ARQ, $ origin, 1;
read ARQ, $ buffer, $ size;
QRA print $ buffer;
close (FILE);
close (QRA);
```

This code is capable of removing specific sections of a binary file and write the removed data in an indicated file.

Table 2 - Archives before the merge procedure.

File	Header	Data
A1	A1header	A1data
A1C	A1Cheader	A1Cdata

The merge of the files was accomplished by using the PERL code previously presented and resulted in the following files:

Table 3 - Files after the merge procedure.

File	Header	Data
NA1	A1header	A1Cdata
NA1C	A1Cheader	A1data

The result was the ability to open both files, using the passwords referenced by the headers. Access to A1data was allowed using the password stored in A1Cheader, and access to A1Cdata was possible using the password stored in A1header.

The same method was applied to files returned by our collaborators, performed by the application of the following commands:

```
REM Extract header from D0 to H0
perl pedaco.pl D0 H0 0512
Resulting file:
163ed3c23f65cadab78c409ef8bb2f5b

REM Extract data from D1 to OD1
perl pedaco.pl D1 OD1 512 299008
Resulting file:
96e0fbef4764293681f814b1c2fb00a1

REM UNION H0 + OD1 INTO ND1
type H0> ND1
type OD1 ND1 >>
Resulting file:
875a17624f0760af55c4e8bf89b08fec

REM Extract date from D2 to OD2
perl pedaco.pl D2 OD2 512 299008
Resulting file:
408698d4fdf30d94738e67ed1be26c3b

REM UNION H0 + OD2 INTO ND2
type H0> ND2
OD2 type ND2 >>
Resulting file:
ad53ae3632d67121e1a5b150ae4c61c4

REM Extract date from D3 to OD3
perl pedaco.pl D3 OD3 512 299008
Resulting file:
f04c0b0043e80fa2b552c5f30dcf4548

REM UNION H0 + OD3 INTO ND3
type H0> ND3
type OD3 ND3 >>
Resulting file:
f0cf30d25732c2da008e028bbba896ae

REM Extract data from D4 to OD4
perl pedaco.pl D4 OD4 512 299008
Resulting file:
c7225987bc6f96fc271c1428162773e6

REM OD4 INTO UNION H0 + ND4
type H0> ND4
type ND4 OD4 >>
```

```
Resulting file:
1941df3165b4f32ca6358ffbaed2900b

REM Extract data from D5 to OD5
perl pedaco.pl D5 OD5 512 299008
Resulting file:
8bd72c5d36e171a99b040b2064ca4949

REM OD5 INTO UNION H0 + ND5
type H0> ND5
type ND5 OD5 >>
Resulting file:
f89678fd88896e24a401b997393a7603

REM UNION H0 + OD6 INTO ND6
type H0> ND6
type ND6 OD6 >>
Resulting file:
a426886834cc9a6aa7923998f7807ba3
```

Table 4 - Files received from collaborators merged with the original header (H0).

Result files	Data file	Header file
875a17624f0760af55c4e8bf89b08fec	D1	H0
ad53ae3632d67121e1a5b150ae4c61c4	D2	H0
f0cf30d25732c2da008e028bbba896ae	D3	H0
1941df3165b4f32ca6358ffbaed2900b	D4	H0
f89678fd88896e24a401b997393a7603	D5	H0
a426886834cc9a6aa7923998f7807ba3	D6	H0

After that, all the containers were opened in Truecrypt with the original password 123.

It is important to note that this process is different from the backup procedure and both the backup and the password changes offered by Truecrypt force the creation of a new encoding header.

It is possible to establish that a non-negligible portion of Truecrypt users are vulnerable to this procedure, since some of them do not have sufficient technical knowledge to install this tool by themselves and thus do this with the aid of others.

A report from BusinessWeek in Jan/2011 depicts among other information that about 30% of help desk calls refer to resetting passwords. [12].

The site of the developers of Truecrypt displays information about the problem with password loss and the constantly request by users of procedures to reset it:

"I forgot my password – is there any way ('backdoor') to recover the files from my TrueCrypt volume?"

We have not implemented any 'backdoor' in TrueCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. TrueCrypt does not allow decryption of data without knowing the correct password or key. We cannot recover your data because we do not know and cannot determine the password you chose or the key you generated using TrueCrypt. The only way to recover your files is to try to "crack" the password or the key, but it could take thousands or millions of years..." [4].

Several internet websites guide users on how to create and share a container on an internal network. For this it is necessary that several people have access to the file and password, further exposing users because even after the departure of one of these people in the company and the exchange of passwords, the terminated employee will always have access to the contents of the file by merging the older header to the updated file.

The following images show the contents of some files supposedly protected by Truecrypt that we could access after the procedures discussed.



Figure 9 - Content of a file in D1.



Para criar um novo usuário

\connect postgres

CREATE USER user_name WITH PASSWORD '98801d41c76c7358a7ceb8e1000df8c';

CREATE ROLE user_name;

ALTER ROLE user_name WITH NOSUPERUSER INHERIT NOCREATOROLE NOCREATEDB LOGIN

PASSWORD 'senha' VALID UNTIL 'infinity';

Figure 10 – Content of a file in D2

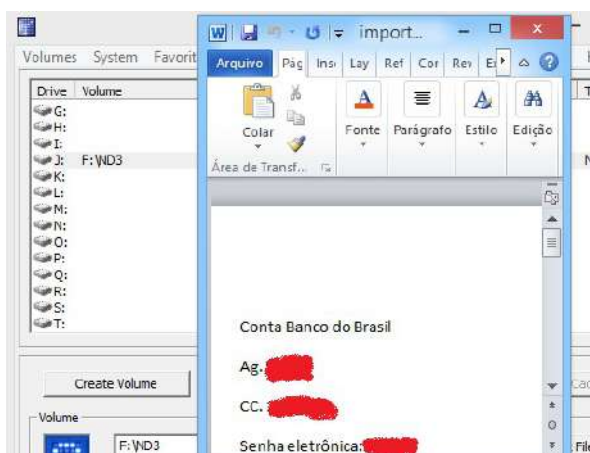


Figure 11 - Content of a file in D3.

```

Na segurança da informação existe uma metáfora, como na corrida da rainha vermelha. No livro "\texti
Para o desenvolvimento de um modelo para detecção de anomalias baseado em aprendizado de máquina, sã
\begin{itemize}
\item Estudar o estado da arte na detecção de anomalias em logs - Compreende na busca e o estudo da
\item Identificar as características para identificar possíveis ataques nos logs - Determinar qual
\item Desenvolver um \textit{parser} para contabilizar e normalizar as características - Desenvolve
\item Desenvolver um classificador utilizando aprendizado de máquina - Desenvolver um classificador

```

Figure 12 - Content of a file in D5.

After the research was conducted, the following information was found on Truecrypt forum, about cloned containers:

“However, since all volumes will share the same key, anyone who knows the password and can open one volume will be able to open all the volumes, even if you subsequently change all the passwords. (All they have to do is use the backup header from a volume that they previously had in their possession.)”[13]

We believe that this information only corroborates with the presented study. The problem with cloned containers and backup headers must be clearly disclosed, because it is easy to notice that it is a common practice among universities to suggest container copy, sharing and header backup. Furthermore, there is no available information that on such circumstances changing the password is not enough to prevent data access with the old one. See [14], [15] and [16].

7 CONCLUSION

The results obtained with the proposed methodology show that sharing containers created by Truecrypt is not a practice that can be validated as safe, since the contents inside then can be obtained by anyone who has access to the original header. Subsequent

password changes do not protect the given contents. The same problem arises from backup headers. We consider that the program remains an important tool, but the functional problem detected must be officially documented (not only in the official forum), given that it causes a profound change in the policy of its usage.

Corporations who use this tool should update their procedures related to the corporate security policy in order to ensure that all internal users understand the limitations presented.

REFERENCES

- [1] KNUDSEN, L. R. Contemporary Block Ciphers. Lecture Notes in Computer Science Volume 1561, 1999, pp 105-126.
- [2] THOMAS, R. Attacks on PGP: A User's Perspective. SANS Institute InfoSec Reading Room. Available at: <https://www.sans.org/reading-room/whitepapers/vpns/attacks-gpg-users-perspective-1092>. Accessed at: 25 apr 2014
- [3] SCHNEIER, B. Attack Trees. Dr. Dobbs's Journal. December, 1999. Available at: <https://www.schneier.com/paper-attacktrees-ddj-ft.html>. Accessed at: 25 apr 2014.
- [4] TRUECRYPT FOUNDATION. Available at: <http://truecrypt.org>. Accessed on: 15 feb 2013.
- [5] Not even FBI was able to decrypt files of Daniel Dantas. Available at: <http://g1.globo.com/English/noticia/2010/06/not-even-fbi-can-de-crypt-files-daniel-dantas.html>. Accessed on: 25 mar 2013.
- [6] Petrobras afirma que informações sigilosas foram furtadas. Available at: http://g1.globo.com/Noticias/Economia_Negocios/0,,MUL298824-9356,00-INFORMACOES+SIGILOSAS+SAO+FURTADAS+D+A+PETROBRAS.html. Accessed on 12 may 2013.
- [7] MOREIRA, D. Roubo de notebook custa mais de US\$ 115 mil. Info Magazine Online. Available at: <http://info.abril.com.br/noticias/ti/roubo-de-notebook-custa-mais-de-us-115-mil-23042009-11.shl>. Accessed on: 12 mar 2013.
- [8] CUNHA, D. F. S. Criminalidade Organizada: antigos padrões, novos agentes e tecnologias. Ponto Urbe. 8. ed. Available at: <http://www.pontourbe.net/edicao8-circula/186-criminalidade-organizada-antigos-padroes-novos-agentes-e-tecnologias>. Accessed on 12 may 2013

[9] Como funciona o PCC - Primeiro Comando da Capital. Available at: <http://www.institutomarconi.com.br/pcc.htm> Accessed on 12 may 2013.

[10] Pesquisa: Gestores de TI admitem vasculhar e-mails privados de funcionários. Available at: <http://computerworld.uol.com.br/seguranca/2007/05/29/igdnoficia.2007-05-29.8374230723/> Accessed on: 12 may 2013

[11] AGGARVAL, G. BURSZTEIN, E. JACKSON, C. BONEH, An Analysis of Private Browsing Modes in Modern Browsers. USENIX 2010, Available at <http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf>. Accessed on 30 jun 2012.

[12] The Problem with Password. Bloomberg BusinessWeek. Available at: http://www.businessweek.com/magazine/content/11_06/b4214036460585.htm Accessed on : 25 mar 2013.

[13] TrueCrypt Forums. Available at: <http://forums.truecrypt.org/viewtopic.php?p=82227#82227> Accessed at: 20 apr 2014.

[14] The University of Manchester. Laptop Encryption. Available at: <http://www.itservices.manchester.ac.uk/secure-it/encryptionsw/laptopencryption/>. Accessed at: 25 apr 2014.

[15] University of Exeter. Available at: <https://as.exeter.ac.uk/it/infosec/encryptionforlaptops/usingtruecrypt>. Accessed at: 25 apr 2014.

[16] Wake Forest University. TrueCrypt Install. Available at: <http://users.wfu.edu/yipcw/is/truecrypt/>. Accessed at 25 apr 2014

Apoc@lypse: when the anti-malware is sick.

By Rogerio Winter, lieutenant colonel at Brazilian Army and Rodrigo Ruiz, researcher at CTI Renato Archer.

Are you sure that your systems are protected?

Several countries recognize that cyber threats can reach a national threat threshold leading to a state that prevents prosperity, security and stability. Notably, the anti-malware and antivirus systems have played a key role, just over 30 years in the defense of several companies' information systems, government and military. However, the anti-virus systems has suffered a large number of critical due to the efficiency of these. In 1987, Fred Cohen demonstrated that no algorithm could detect perfectly all the possible viruses. This was a very discouraging observation when we thinking about antivirus. Other people recently declared, "Antivirus is dead".

The antivirus concept was changed to the anti-malware concept, however antivirus is the most widely known. Inside the anti-malware is embedded a threat detection system which the signature-based technology is one of the most popular technologies against virus and malware.

The different anti-malware software makers announce new and efficient technologies that claim to offer better performance and cheaper answers us with malware security incidents within organizations. Clearly, there can be a technology that is faster, better and more efficient than all others. Our research went back to the basic beginnings, to the DNA of the antivirus. We questioned the paradigms now consolidated in the software through four decades, revised the history of the development of this software, and started to carefully study the common nucleus. Making an analogy to the human body, the fault is in the DNA of the ancestors of the modern antivirus software.

The use of terms like infection, incubation, and disease in the context of information security suggests a similarity between computers and biological virus, a logical parallel. The similarity between the virtual world and the reality is notable. Solutions to fatal computer problems were inspired by the observation of nature itself. In this way, we can establish a metaphor between human body and cyber body, particularly of the system protect. An autoimmune disease occurs when the human immune system has a fault, and it attack cells and tissues of the organism itself in the same way as a virus or a bacterium tries to infect a human body.

All the antivirus software on the market have the same algorithms in common. In other words, the methodology that compares signatures of the virus was created almost three decades ago. The virus classification is made by signature without considering the behavior of the virus.

What is not Apoc@lypse Technique?

The Apoc@lypse Technique is not a malware. Malware is malicious software that infect computers; however, they have a more limited range in terms of operating system, anti-malware vendor and time.

What is Apoc@lypse Technique?

We call the first autoimmune cyber disease, because the Apoc@lypse technique is a trigger for start the autoimmune disease in computer. Autoimmune disease in human is a disease in which a person's immune system wrongly attacks its own healthy tissues. The Apoc@lypse technique is a generic and extremely efficient way to bypass the protection of the anti-malware system. The technique explore a vulnerability that exist in the signature-based technology of the anti-malware and it allows infecting in the furtive form a machine target. We injected tens and hundreds of malware pieces of DNA known benign files in the system itself without any action of anti-malware. All file types are susceptible to action infection the Apoc@lypse technique, such as file system, user system or software. We can use any part of the malicious DNA and some antivirus will be affected and others not. However, a special DNA affects all antivirus. This is EICAR Anti-Malware Testfile, because all antivirus recognize it as a virus or malware but this is not a virus. The test file simply displays a text message and returns the control to the operating system. After infection, the anti-malware system started autoimmune cyber disease and all files infected was deleted from system.

The signature and hash identify and distinguishes the appearance, and not the attitude, of software. Even the heuristic concept carries with it the detection of several indicators of a signature or stereotype of a threat. The Apoc@lypse Technique is implemented in software and it allows choosing between several existent forms of infection.

Apoc@lypse Technical Potential

Anti-malware system are inefficient when we use Apoc@lypse Technique against system. The Apoc@lypse Technique undoubtedly will contribute to bring the system into more disrepute and discouraged users from using it. According to, The Global State of Information Security® Survey 2014 of PWC , the companies have invested in cyber security, but they are not accompanying the evolution of his current adversaries. Nowadays, we are trusting in model security created in the past to struggle present threats.

Proof of concept

We demonstrated that is possible to take control of anti-malware system and to command operating system destruction. The Apoc@lypse Technique proof of concept is more effective in Windows Operational System, but for the other operational systems (Linux, Android, UNIX e Mac) the effects can be less catastrophic. The Apoc@lypse technique explore undisclosed vulnerability in the anti-malware systems. Technical efficiency of Apoc@lypse were successfully tested in 157 anti-malware system existing in the international market. In figure 1, we present the geographical distribution of anti-malware companies in the world used in Apoc@lypse test bed. The technique Apoc@lypse is efficient in various versions of Operational System Windows 32 and 64 bits.

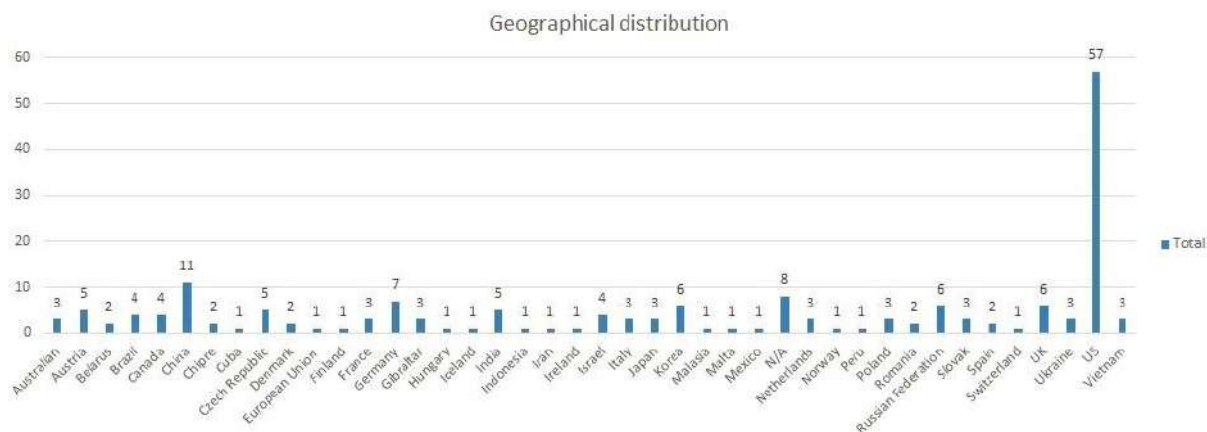


Figure 1 Geographical distribution anti-malware companies in the world. Source: authors.

Apoc@lypse technique corresponds to the end of the systems of signatures and hashes to identify threats against the security of information, since the system distinguishes and identifies the appearance, and not the attitude, of software. Even the current heuristic concept carries with it the detection of several indicators of a signature or stereotype of a threat.

How will Apoc@lypse influence the defense of military systems, bank systems, and controllers of infrastructure? As common systems are weakened, too many systems use computers with antivirus and anti-malware protection, and it may cause an avalanche and compromise the functioning of too many systems.

About the Authors



Rogerio Winter is a signals officer in the Brazilian Army who occupied multiple positions in network administration, command and control, electronic warfare, and cybersecurity. He received his master degree in Electronic Engineering and Computer Science from the Institute of Aeronautical Technology (ITA), Brazil. Currently, he is an Army Liaison Officer at the Center for Information Technology Renato Archer, Government Advisory Committee in IT-SA Brazil, and book's coauthor "Apoc@lypse: the end of antivirus".



Rodrigo Ruiz has discovered the vulnerability Apoc@lypse and carried out a digital bacterium to transport and inoculate the DNA of viruses in computational systems. He was the first one to draw the parallel between autoimmune cybernetics and disease, which is the basis of this book, and he created the proofs of concept. Rodrigo is book's coauthors "Apoc@lypse: the end of antivirus" on.

Apoc@lypse: The End of Antivirus

Rodrigo Ruiz

Rogério Winter

Kil Park

Fernando Amatte

We are grateful to pixabay.com and Isabela Ganzert Ruiz for the images.

We are grateful to CreateSpace.

Technical Revision

Kil Park

Rogério Winter

Rodrigo Ruiz

Fernando Amatte

Organization and Research

Rodrigo Ruiz

Codes

Rodrigo Ruiz designed all codes in this book.

Fernando Amatte created code to accelerate the development of bacterium packer system.

Chapters by Author

Rodrigo Ruiz wrote chapters 6, 7 8, 9, and 10, coauthored by Rogério Winter.

Kil Park wrote chapters 2, 3, and 4.

Rogério Winter wrote the Introduction and chapters 1, 11, and 12, coauthored by Rodrigo Ruiz.

Fernando Amatte wrote chapter 5.

Translation to English

Rogério Winter

Copyright © 2015 by Victoria Ganzert

All the rights reserved.

No part of the book may be reproduced in any form, by photostat, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, without the written permission of the copyright owner.

ISBN: 1514863677

ISBN-13: 978-1514863671

Library of Congress Control Number: 2015912081

LCCN Imprint Name: CreateSpace Independent Publishing Platform, North
Charleston, SC

Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode.

Rodrigo de S. Ruiz ¹, Fernando Pompeo Amatte, Kil Jin Brandini Park D. Sc. ², Rogério Winter ³

1 Malware Analysis Nucleus (NUCAM)
Renato Archer Information Technology Center (CTI)
Campinas – SP, Brazil.

2 Computer Faculty (FACOM) –Federal University of Uberlândia
Monte Carmelo – MG, Brazil

3 Brazilian Army

rodrigosuiz@outlook.com, famatte@gmail.com, kil@facom.ufu.br, rogwinter@gmail.com

Abstract — A growing concern of users about confidentiality and privacy in web related tasks presses companies to present more secure solutions that respect the right to individual privacy. However, as some sources show, the most common browsers on the market are not able to maintain adequate privacy, even with the adoption of private browsing mode. For law enforcement agents this vulnerability may give a chance to acquire evidence during an investigation. Information security or lack of it solidifies into issues that often are not technical. The first concept is the confidence. Conceptually, trust is the firm belief that one has in relation to another person or something. Certainly, several security incidents began in the confidence that software and hardware would not fail under certain conditions. This paper presents a data capture method of browsers related activities and argues that it is possible to recover text and graphics data related to pages visited during private browsing sessions. The observations, reported in this article, show a clear violation of the functional requirement to maintain user's privacy. Overall, it is important to assess and validate private browsing techniques.

Keywords: Privacy, Private browsing, Browser safety, Browser forensics.

1. INTRODUCTION

“Security is a feeling of protection, necessary and indispensable to a society and each of its members, against threats of any kind”. Defense is the capable action to sustain security feeling [1].

From this concept, we can derive issues pertaining to technology, software, quality and reliability of the environments and systems that need to protect critical information. Information security depends on the reliable operation of the infrastructure, which in its nature is critical. Cyber threats exploit the growing complexity and connectivity of critical infrastructure systems, putting safety at risk.

Information security or lack of it solidifies into issues that often are not technical. The first concept is the confidence. Conceptually, trust is the firm belief that one has in relation to another person or something. Certainly, several security incidents began in the confidence that software and hardware would not fail under certain conditions.

On this point, the paper discusses a security breach in the private mode function of browsers, which starts as social process of confidence. Logically, the information provided by the developer is considered reliable. It is usually not questioned or simply accepted as true.

Therefore, this article is aimed at answering the following questions:

- Can privacy be guaranteed when the browsers are used in private mode?

- Can the data acquisition methodology used for testing be considered efficient for evaluating privacy aspects?

Our work focuses on checking the status of privacy provided by browsers. As mentioned earlier, trust is a social process that may at some point be abused. For the study, we collected statements of developers on the use of private browsing and the consequences of its adoption to user's privacy.

In this work, we present the following contributions in the privacy area of research: a collection and analysis method for data generated by browsers and web navigation and fault identification in the chain of privacy. The generic method of collection and analysis contributed significantly to the given conclusions about the limits of the private browsing functionality. Moreover, we could analyze and identify possible flaws in the chain of privacy, from aspects ranging to the knowledge collected by the operating system through the implementation and use of the private browsing mode in browsers.

This paper is an extended version of a work previously presented by the authors [2], with additional results and analysis, and it is structured in the following topics: introduction, our contribution, related works, method and tests, results, discussion, conclusion, and references.

2. CONCEPT ABOUT PRIVACY

Currently, privacy concerns have gained a prominent place in people's lives; however, the behavior in respect to privacy is different. Dienlin's work [3] discusses in depth the privacy concerns that people have and behaviors relating to privacy that are adopted.

The privacy issue on the internet is sometimes controversial and difficult to solve. Therefore, privacy is not only achieved with the use of software tools, but also with a change of attitude on how to access information on the internet.

This change in attitude is the cornerstone to achieve the desired privacy. When seeking anonymity or privacy on the internet the principle goes beyond the use of technological tools. A user when browsing on the internet is basically subject to the following elements that can monitor their

habits and customs: LAN administrator, internet service provider, operating system and other applications on the computer and site services:

1. Local network administrator - a network administrator can identify internet users habits due to the available technological resources in a router and other net devices. This way, the administrator can trace user profiles, monitor network traffic and other operations.
2. Internet service provider – in the same way as the LAN administrator, the service provider can access information from users and their preferences.
3. Computer operating system - There is no software immune to errors caused by incorrect coding or hardware failure. With that in mind, software developers many times include software routines to measure and store telemetry related data based on the software execution. This information sometimes can be sent to the developer independent of the will of the user. A malicious developer may use this information in an incorrect manner or may even sell this information to interested third parties.
4. Site on the internet - for a service to be profitable on the internet, the owner of the system must constantly assess the profile of its customers. Thus, access monitoring is a mandatory activity to establish consumer habits and geographic users' location.

The goal of software testing is to show the presence of defects if they exist [4]. Similarly, the goal of our work is to identify possible weaknesses in browsers that can compromise the privacy of users.

On the one hand, such a feature, if operating perfectly aligned with security guidelines, provides the user privacy in their online activities. On the other hand, it is clear that in case of unlawful behavior, law enforcement officers have to deal with this layer of protection to obtain the necessary data to provide evidence during the course of an investigation.

In both cases, it is important to verify the actual functionality of such a feature, if available implementations actually provide the degree of confidentiality offered, or if there are flaws that allow the retrieval of online activity data.

3. RELATED WORKS

Aggarwal et al. [5], establishes a definition of the attack model between site attacker and web attacker. Moreover, the study is based on a technique where they discover how to remotely test if a browser is currently in private browsing mode. Finally, they describe an automated technique to identify failures in private browsing implementations and used it to discover a few weaknesses in the Firefox browser. The deepest analysis was conducted in Firefox 3.5. They primarily focus their analysis on the Firefox browser where the testing of private browsing mode has been done by conducting the MozMill tests.

In Mahendrakar et al. [6], the analysis was performed to collect evidence of some standard tests. They created a website that contained individual pages which required the browser to interact with some forms. The authors used virtual machine VMWare Workstation 6.5 to perform the tests. They analyzed the existing content in virtual memory after using the browsers Firefox, Internet Explorer, Chrome and Safari.

Chivers [7] presents a study based on Internet Explorer 10, particularly about the InPrivate Browsing. The author pointed out that this version of Internet Explorer marked a profound shift in the way internet history and cache memory data are stored within the file system. The system was replaced with a high performance database technology known as the Extensible Storage Engine (ESE). This paper reports the results of the experiment performed on the Windows desktop 8. He discusses some implications for seizure tactics where the evidence can be found on the increasingly complex data structures used to record the activity on the internet. The prospect of recovery of such evidence, together with its potential forensic importance, raises questions, including where and when such evidence can be retrieved, so you can prove that a recovered artifact originated of an InPrivate browsing session.

In their article Ohana and Shashidhar [8], also working with Internet Explorer 8 among other browsers discovered residual artifacts from private and portable web browsing sessions. Portable web browsing artifacts are primarily stored where the installation folder is located (removable disk). Their testbed was composed of Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome, but they used Microsoft Windows 7 Professional 64 bits.

4. METHOD AND TESTS

When testing a security feature, it is necessary to define its functional requirements and the profile of the attacker who will try to disable or override this feature.

A paper on the analysis of private browsing functionality [5], lists the profiles of potential attackers, security models to be checked and the objectives to be met by browsers that implement private browsing.

One must understand that when privacy is important, any element pertaining to the set of resources used could be responsible for leaking private data. In this respect, any browser plug in must be compliant with the security policies in use:

“Browser plug-ins and extensions add considerable complexity to private browsing. Even if a browser adequately implements private browsing, an extension can completely undermine its privacy guarantees” [5]

Also noteworthy is that attackers could be either local or remote. In the first case, one has physical access to the user's machine while in the second one can only launch attacks through network connections.

Furthermore, according to [5] we can classify the changes caused by user's navigation actions in four different categories:

1. Changes caused by web site independent of the user actions, e.g. caching.
2. Changes caused by web site but dependent of the user actions, e.g. adding a certificate.
3. Changes caused directly by user actions, e.g. adding data to a form field.
4. Changes caused by other sources, e.g. updating the browser.

Changes pertaining to any category could be the source of a breach on private browsing.

In this work, we start from the methodological framework presented by [5], for the construction of the following methodological model:

The profile of the attacker considered assumes that he has local access to the user machine. Consequently, attempts to circumvent the system of private browsing will occur from an image taken from the user's machine hard drive.

As the focus of the evaluation is the private browsing feature, we considered that the user does not adopt other security tools or techniques that could exert influence on the access of the data generated during navigation.

As an example of such influence, [9] considers the impacts on forensic evaluation caused by the adoption of cryptographic methods in the disk of the user's machine. In the case of file level cryptography (or the use of encrypted containers), as those mechanisms are not fully integrated with the operational system, they are not able to prevent activities from generating sensitive data outside the containers or files protected, such as application data found on temporary files or even on swapping and paging structures on the file system.

This level of protection is only achieved with the adoption of full disk encryption (FDE). In this case, turning off the target machine and cloning its hard drive may not be the best approach, because the entire hard drive contents will be protected and the forensic analyst will need the passphrase or cryptographic key to access then. Given the circumstances, [9] points that forensic analysts should consider performing live system forensic when possible in systems where FDE is applied.

When performing forensic analysis of browsers, one can consider the specific artifacts such as data structures and files or implementation characteristics of each one of them or perform a browser independent forensic analysis of the entire file system searching for significant data.

Proposing a new tool for browser forensic analysis, [10] present a list of browser structures that could be targeted, such as history, cookies, download lists, bookmarks, cache and index.dat file. Furthermore, they propose a methodology to extract search history of search engines used in the browsers by users through the application of signatures derived from the study of HTTP URL generated from those searches.

However, this paper focus on searching the user's machine for fragments of data from which text or images that brings information about pages visited

could be extracted. Therefore, the specific analysis of changes to files used by browsers such as history, cookies, cache and certificates was not performed. Specific analysis of those characteristics can be found in [5], [10], and [6].

We performed two different test batches. In the first batch, four different set of actions were performed on the browsers Internet Explorer [11], Firefox [12], Google Chrome [13] and Safari [14].

We tested Internet Explorer browser on bare metal hardware with the use of four notebooks equipped with Windows 7 Pro SP1.

For the other tests performed, we created a standard guest virtual machine - with the operating system Windows 7 Pro - in the host operating system - Windows 7 Pro - using the virtualization software Virtual Box [15].

An export (snapshot) of the newly installed Windows machine was created, considering the possible need for future comparison of the base guest machine with guest machines running the different browsers tested.

The browsers tested were Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1 and Safari 5.1.7_1. The base guest virtual machine for each browser was replicated 4 times, each to be used in the four different tests performed on each browser.

Based on those configurations, the four different set of actions were applied for each browser in private browsing mode:

Table 1: Test Type

Test Type	Action
S (Shutdown)	Consists of visiting a web site available on the internet, making operations to interact with the site, finish the execution of the browser correctly and generating the virtual machine image for analysis. This test is the most favorable for both the operating system and the browser because the user follows the steps expected for the shutdown of the machine.
F (Freeze)	Consists of visiting a web site available on the internet, making operations to interact with the site and with the browser still active, generating the virtual machine image for analysis.
K (Kill process)	Consists of visiting a web site available on the internet, making operations to interact with the site, requesting that the operating system interrupt the browser execution and generating the virtual machine image for analysis.
P (Power down)	Consists of visiting a web site available on the internet, making operations to interact

with the site, requesting the virtualizer to turn off the virtual machine - simulating a power outage - generating the virtual machine image for analysis.
--

In the second test batch, we only applied one set of actions, represented by Test S, for the browsers TOR Browser Windows 3.6.6 [16] and Safari 6.0.3 (8536.28.10).

The TOR browser test was conducted on a guest operating system Windows 7 Pro SP1 running over a Virtual Box [15] virtual machine.

The Safari test happened on MAC OS Mountain Lion, 10.8.3 running as guest on a VMWare [17] virtual machine.

For each test performed, the virtual machine image generated is analyzed through the application of the program Strings [18] found in many different Linux distributions.

This program is used for the search of strings inside the virtual machine images that could present relation to the webpage visited.

The images of the virtual machines are also analyzed for the search of graphic files associated with the visited webpage, through the usage of the Foremost program [19], a renowned forensic tool for extraction of files - "data carving" - of different formats.

A study about data analysis inside the Windows pagefile, [20] points out that for data extraction the two approaches represented by both tools (Strings and Foremost) have differences but are considered standard inside the forensic analysis field.

About the process of file carving, one can generalize the method as:

"By using a database of headers and footers (essentially, strings of bytes at predictable offsets) for specific file types, file carvers can retrieve files from raw disk images, regardless of the type of filesystem on the disk image." [21]

In other words, the foremost tool works as follows: It reads a block of data - memory, disk or files - and looks for signatures (headers or footers) related to files of well-known formats. It is noteworthy that in the present research we investigated only the persistent memory (i.e. physical and virtual disk).

Since these signatures are a sequence of bytes, there is the chance of occurrence of false positives and therefore the capture of incorrect file.

Furthermore, it is important to note the existence of several known problems associated with the use of

tools aiming for "data carving", for example, limitations to the treatment of non-contiguous data. Thus, it is possible for an image whose sequence of bytes is dispersed to not be fully recovered, despite its possible existence in the block of data analyzed.

About the Foremost software, it is also possible to measure its acceptance and support in the digital forensic community through the analysis of many studies where it was applied.

In one such paper about the forensic analysis of the XBOX videogame system, [22] discusses that the use of Foremost could speed up the carving of data of XBOX executable files ("xbe" type).

While discussing different forensic techniques for mobile Windows phone analysis, [23] compares the carving performance (with comparing metric given by numbers of artifacts detected, partially or fully recovered) of the data carving programs Scalpel, Foremost, Simple File Carver and Phone Image Carver.

To test a proposed methodology to compare file carvers, [24] chooses the following tools: Foremost, Scalpel, PhotoRec and Adroit. Their conclusion based on the results obtained was that the best approach is to use various tools in order to explore the strong points of each one and to perform file validation tests after the data carving tools processing.

One last important comment about the choice of Foremost is that it is an open source tool. As any forensic evidence that could potentially be used in a court of law, it is of paramount importance for the evidence to be deemed as legally valid. To that end, the tools used in the process should clearly follow any legal guidelines pertinent to evidence reliability. And as one study points out, under the Daubert test guidelines, "...open source tools may more clearly and comprehensively meet the guideline requirements than would closed source tools." [25]

The WinHex tool [26] was also used to search for keywords found in the navigated webpage.

5. RESULTS

Aiming to simulate an actual visit to any website available on the internet, a random selection was made, and the sites chosen for the experiment was [27] and [28]. Since some site information is proprietary, the figures recovered during the test will be only partially reproduced in the present work. We would like to acknowledge that those

information are copyright of their respective owners.

First Batch of Tests – Four Different Set of Actions

SAFARI Browser

For the Safari browser, the following results were obtained:

F test (freeze)



Figure 1 - “storage.discovery.com” string located in virtual machine’s image.

No image fragments were found on the virtual machine’s hard disk image.

K Test (kill process)



Figure 2 - “discovery.com” string located in virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 3 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage visited:

p://dsc.discovery.com/videos
http://store.discovery.com/?ecid=PRF-DSC-101345&pa=PRF-DSC-101345

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 4 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited:

http://store.discovery.com/discovery/layout/favicon.ico
http://dsc.discovery.com/
http://games.dsc.discovery.com/
http://dsc.discovery.com/tv-shows
http://store.discovery.com/discovery/layout/favicon.ico

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 5 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage visited:

http://dsc.discovery.com/tv-shows
http://dsc.discovery.com/
http://store.discovery.com/discovery/layout/favicons.ico
http://dsc.discovery.com/videos
america.discovery.com.edgesuite.net
velocity.discovery.com
metrics.discovery.com
orate.discovery.com
animal.discovery.com.edgesuite.net

The results obtained for the Safari browser tests are grouped in table 1:

Table 2 – Results for Safari Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

FIREFOX browser:

F Test (freeze)

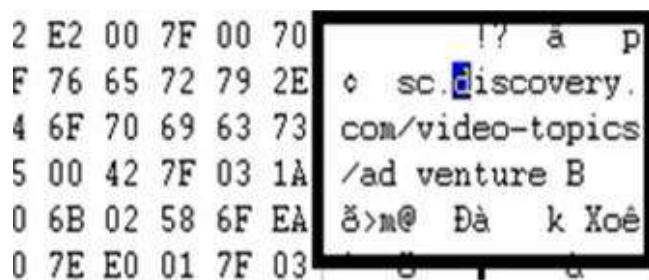


Figure 6 – “sc.discovery.com/video-topics” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test (kill process)

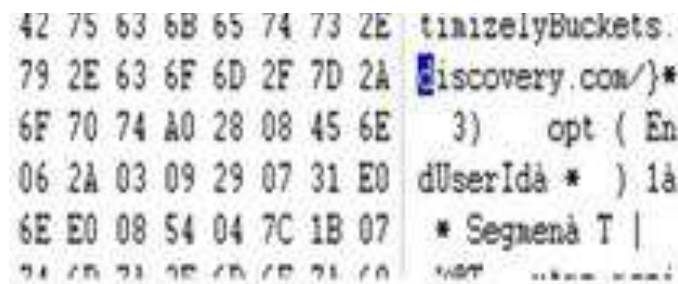


Figure 7 – “discovery.com” string located in the virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 8 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage visited:

C:\Program Files\Mozilla Firefox\firefox.exe
ttp://games.dsc.discovery.com/
/ttp://dsc.discovery.com/videos
http://games.dsc.discovery.com/word-games
http://games.dsc.discovery.com/sport-games
https://securestore.discovery.com/cart.php
https://securestore.discovery.com/cart.php
store.discovery.com
http://games.dsc.d

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 9 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicates the webpage visited:

```
investigation.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
netstorage.discovery.com.edgesuite.net
games.dsc.discovery.com
```

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 10 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage visited. A fraction of strings retrieved in this test follows:

```
Fdsc.discovery.com%2Fvideo-
topics%2Fadventure&u=oeu138176054536
Or0.4355827774372748&wxhr=true&t=138
1760579498&f=340937086
http://dsc.discovery.com/
h;e++)if(a[e].name=="keywords")if(b=
==""))b=a[e].content;else b+=",
"+a[e].content;else
if(a[e].name=="description")c=a[e].content
;if(!(b.length+c.length>eb)){z("dmk",b);z("d
md",c)}}function ub(){var
a="__cmb",b=[];for(var c in
aa)c.indexOf(a)==0&&b.push(c)
```

*s_sess=%20s_cc%3Dtrue%3B%20s_campai
gn%3DPRF-DSC-101345%3B%20s_sq*

Table 3 – Results for FireFox Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

GOOGLE CHROME Browser

F Test (freeze)

Some strings related to the webpage were also found in hard disk analysis:

```
3A 2F 2F 64 73 63 2E 64 10 http://dsc.d
2E 63 6F 6D 2F 00 31 20 iscovery.com/ 1
D6 4D B5 F9 E0 75 77 07 = v0!e0Mpuauv
06 20 03 40 00 07 F6 71 %o @ oq
3F A0 00 07 7C 3B 6F 68 6i!e? |.oh
D2 71 6E 90 69 64 00 03 o) Uqn id
E0 11 7F 80 1F 0C D6 D2 tio' a | 00
70 07 AD 20 7F 40 E7 01 !eV à Jp - @c
F1 F5 76 02 48 F9 6F 6C !eà & v!E3v Hùol
```

Figure 11 - “http://dsc.discovery.com” string located in the virtual machine’s image.

```
74 65 49 45 38 22 3E 64 e="EmulateIE8">d
74 69 6F 6E 2E 63 6F 6D investigation.com
3E 0D 0A 20 20 20 20 3C </domain> <
69 73 63 61 73 2E 6E 65 domain>discas.ne
6E 3E 0D 0A 20 20 20 20 t</domain>
64 69 73 63 6F 76 65 72 <domain>discover
6F 6D 61 69 6E 3E 0D 0A y.com</domain>
61 69 6E 3E 64 69 73 63 <domain>disc
64 6F 6D 61 69 6E 3E 0D uz.net</domain>
6D 61 69 6E 3E 64 69 78 <domain>dix
6B 3C 2F 64 6F 6D 61 69 oas.co.uk</dowai
```

Figure 12 - “discovery.com< /domain>” string located in the virtual machine’s image.

K Test (kill process)

```
6C 69 66 69 65 64 55 52 fullyQualifiedUR
2F 2F 64 73 63 1F 2E 64 L:"http://dsc d
2E 63 6F 6D 2F 74 76 2D iscovery.com/tv-
72 76 69 76 6F 72 03 6D shows/survivor a
62 75 72 6E 2D 62 61 62 an/^ s/burn-bab
6D 22 2C 64 75 72 61 74 v-@ .hta".durat
```

Figure 13 – “discovery.com/tv-shows” string located in the virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:

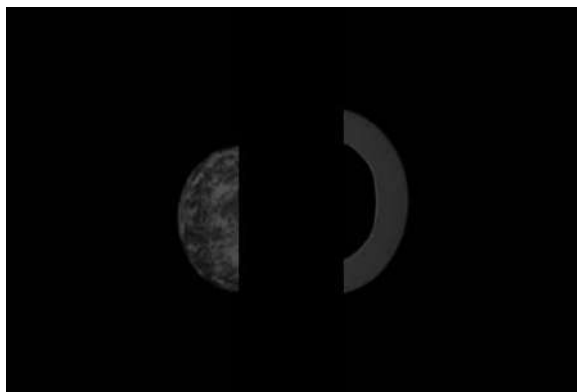


Figure 14 – Image recovered on hard disk image analysis and found on Discovery.com website.



Figure 15 – Image recovered on hard disk image analysis and found on Discovery.com website.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 16 – Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage visited. A fraction of strings retrieved in this test follows:

```
//dsc.discovery.com/  
://static.ak.facebook.com/connect/xd_arbi  
ter.php?version=27#cb=fdde13148&domain
```

```
=dsc.discovery.com&origin=http%3A%2F  
%2Fdsc.discovery.com%2Ff2a7e0cd34&rel  
ation=parent&error=unknown_user  
/dsc.discovery.com/tv-shows  
://dsc.discovery.com/  
://dsc.discovery.com/  
://dsc.discovery.com/  
http://dsc.discovery.com/tv-shows  
http://dsc.discovery.com/tv-shows  
http://dsc.discovery.com/
```

S Test (Shutdown)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 17 - Image recovered on hard disk image analysis and found on Discovery.com website.

The strings utility could also recover text references in the virtual machine hard disk image analysis that indicated the webpage was visited. A fraction of strings retrieved in this test follows:

```
": "Survivorman  
Videos", "srtUrl": "", "uuid": "8e18dcd9-8d1d-  
11e2-a7b7-06a90ff35868", "bdat": "must  
watch", "keywords": "survivorman, 10  
days, ten, days, must  
watch, mexico, tiburón, deserted, island, les  
stroud, survival, survivor, man, water, pool, alg  
ae, fresh, cane, reed, sludge", "mediaType": "lift  
", "mp4": [{"bitrate": "110k", "src": "http://disc  
smil.edgesuite.net/digmed/hdnet/07/a7/1377  
6400801197_102MissingPiece-  
110k.mp4"}], "akamaihd.net/i/digmed/hdnet/9  
8/9a/13776401201197_104Stove-  
, 400k, 110k, 200k, 600k, 800k, 1500k, 3500k, .mp  
4.csmil/master.m3u8", "networkId": "DSC", "t  
humbnailURL": "http://netstorage.discovery.  
com/feeds/brightcove/asset-  
thumbnails/dsc/0a5dbdfa893fec1f556a7d81c
```

5b28bc470ecbb0e_0a5dbdfa893fec1f556a7d
81c5b28bc470ecbb0e.jpg"

Table 4 – Results for Chrome Browser

	F Test	K Test	P Test	S Test
Page address recover	Yes	Yes	Yes	Yes
Picture recover	No	Yes	Yes	Yes

INTERNET EXPLORER Browser

F Test (freeze)

```

35 00 33 00 41 00 25 00 25 00 32 00 35 00 32 00 25 2 F % 2 5 2
2E 00 64 00 69 00 73 00 F d s c . i s
72 00 79 00 2E 00 63 00 c o v e r y . c
35 00 32 00 46 00 66 00 o a % 2 5 2 F f
35 00 38 00 33 00 33 00 2 2 a 3 5 8 3 3
36 00 32 00 25 00 32 00 1 2 4 3 6 2 % 2

```

Figure 18 – “discovery.com” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

K Test (kill process)

```

B2 00 01 68 00 74 00 74 00 73 00 74 00 6F 00 72 00 73 00 63 00 6F 00 76
00 63 00 6F 00 6D 00 2F 00 6A 00 61 00 78 00 2F 00 44 00 65 00 74 00 61
00 2E 00 32 00 2E 00 6A 00 72 00 3D 00 31 00 30

```

Figure 19 – “http://store.discovery.com/js/ajax/” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis.

P Test (Power down)

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 20 – Image recovered on hard disk image analysis and found on Discovery.com website.

S Test (Shutdown)

On this test, another step taken was the analysis of log files generated by the Internet Explorer browser. It is easy to see that the page address is easily visible inside a log file:

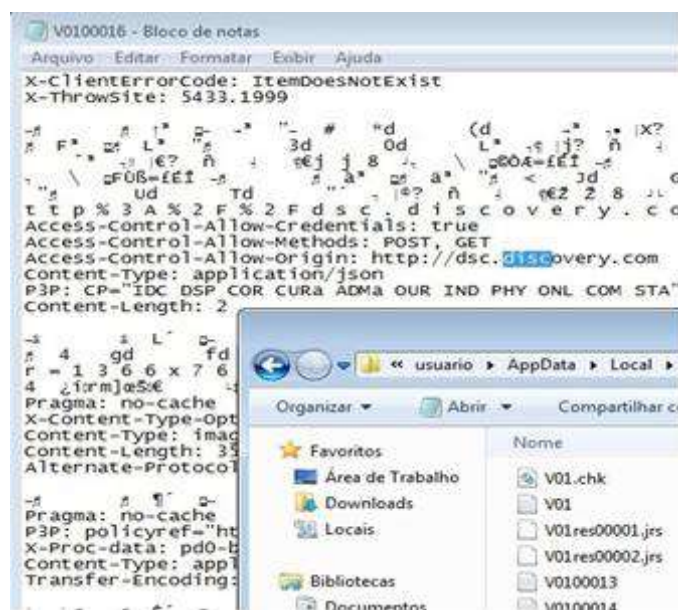


Figure 21 – Log file found using only the explorer and notepad. They demonstrate the system failure (string http://dsc.discovery.com found) in the private-IE10.

Table 5 – Results for IE10

	F Test	K Test	P Test	S Test
Page address recovery	Yes	Yes	No	Yes
Picture recovery	No	No	Yes	No

Second Batch of Tests – One Set of Actions

TOR Browser


```
63 6F 76 65 72 | discover
27 00 65 00 88 | y.com 0l' e l
00 65 00 72 00 | n s I O b s e r
27 00 72 00 88 | v e r 0l' r l
00 00 00 00 00 |
```

Figure 22 – “discovery.com” string located in the virtual machine’s image.

```
20 3A 20 22 64 | title : "d
63 69 65 6E 63 | iscovery: scienc
20 73 70 61 63 | e. history. spac
61 72 6B 73 2C | e. tech. sharks.
```

Figure 23 – “discovery: science, history, space, tech, sharks” string located in the virtual machine’s image.

Images related to the webpage visited were found on the virtual machine hard disk image analysis:



Figure 24 – Image recovered on hard disk image analysis and found on Discovery.com website.

SAFARI Browser

```
00 2F 00 77 00 | h t t p : / / w
00 74 00 6F 00 | w w . h i s t o
00 2F 00 66 00 | r y . c o m / f
00 2E 00 69 00 | a v i c o n . i
09 68 00 74 00 | c o E h t
```

Figure 25 – “http://www.history.com/favicon.ico” string located in the virtual machine’s image.

```
00 2E 00 68 00 69 | / / w w w . h i
00 2E 00 63 00 6F | s t o r y . c o
00 65 00 6F 00 73 | a / v i d e o s
```

Figure 26 – “http://www.history.com/videos” string located in the virtual machine’s image.

No images related to the webpage visited were found on the virtual machine hard disk image analysis. Further analysis to prospect the files and directories involved in the data leakage generated the following results:

In all browsers, some of the data associated with the navigation could be extracted from the file pagefile.sys. This proves that part of the data is leaking through the paging process’s storage mechanism used by the operating system.

In Internet Explorer’s case, more data could be found in a file located at the directory:

`\user\<username>\appdata\local\microso
ft\windows\temporary internet
files\low\content.ie5\ndm4l4gv\`

On Chrome’s case, more data could be found in the file:

`\user\administrador\appdata\local\microso
ft\windows\webcache\webcachev01.dat`

Those files points to the fact that navigation data is leaking from cache files used by the browsers.

In Table 5, we can see a summary of all tests.

Table 6 – Summary

Recovery	F Test	K Test	P Test	S Test	Browser
Page address	Yes	Yes	No	Yes	Safari
	Yes	Yes	Yes	Yes	Firefox
	Yes	Yes	Yes	Yes	Chrome
	n/a	n/a	n/a	Yes	Tor Browse
	n/a	n/a	n/a	Yes	Chrome/ Android 4.0.3
Picture	No	Yes	Yes	Yes	Safari
	No	Yes	Yes	Yes	Firefox
	No	Yes	Yes	Yes	Chrome
	n/a	n/a	n/a	Yes	Tor Browse
	n/a	n/a	n/a	Yes	Chrome/ Android 4.0.3

6. DISCUSSION

After the tests carried out using the proposed methodology, we can return to the issues that gave rise to the current research. Can privacy be guaranteed when the browsers are used in private mode? Can the data acquisition methodology used for testing be considered efficient for evaluating privacy aspects?

In this context, we can discuss two possibilities: the effects of operating system in private mode browsing and the particularities on the implementation of the functionality itself. We understand that certain beliefs may be proven wrong under those two approaches.

In the first case, the software is built upon the operating system abstraction layers, and various functions and system calls required for browsers are imported from the operational system itself. In this way, memory management and I/O operations are under the domain of the operational system removing the browser's power to determine what should be recorded and where on. Without full control of those actions, the browser is dependent on the OS to maintain user's privacy.

In the second case, the browser's domain, the developer creates expectation of privacy in users when they declare that their software has features that are able to prevent others to reconstruct the steps the users took during their online activities. As an example Firefox and TOR Bundle browsers rely on functions that are specific to the Windows operating system.

However, with the possibility of user's privacy loss, as shown in the results gathered on this paper, the statements by the developers about the insurance of user's privacy seem misleading and, therefore, can destroy the trust between the parties.

On the other hand, in the case of the IE, Chrome and Safari browsers developers are the same developers of the operational system, Windows, Android and Mac OS, respectively. For this reason, the developers have condition to fully control and change the system behavior. However, what we see is a situation similar to that covered on the previous paragraph, because even in favorable condition browsers behavior is the same, leaving residues that could allow some form of identification of web browsing habits of users.

All things considered and returning the assumptions that led to the present research, private mode browser functionality is not sufficient to guarantee users' privacy when tested with the article proposed method and boundary conditions.

Finally, we argue that the methodology used in collecting and analyzing the data is valid to evaluate the implementation aspects of private browsing. It allowed the construction of a privacy model that supported the discussions and elucidated the key aspects and assumptions analyzed that ultimately proved problems not only in the implementation of various browsers private

browsing functions but also on the management of resources by the operational systems.

7. CONCLUSION

In all four types of tests performed, it is possible to verify that all browsers tested presented flaws in their private browsing feature.

Those flaws generates data that remain available in the system and allow not only the identification of pages visited but in some cases also to partially rebuild them.

Browsers promises to leave no traces of the navigation activities of users. This work proves that privacy as advertised is not provided.

In face of the results obtained, we would like to recommend the developers to explicitly alert the users about the limitations of the private browsing functionality implementation.

If on one hand this is a negative point for the user, on the other hand those flaws facilitate the work of law enforcers in cases where there is need for the data recovery related to the navigation activity.

8. REFERENCES

- [1] Escola Superior de Guerra, "CAMPOS DE ATUAÇÃO DO PODER NACIONAL," em *Manual Básico da Escola Superior de Guerra - Elementos Fundamentais Volume I*, Rio de Janeiro, Biblioteca General Cordeiro de Farias, 2013, pp. 66 - 84.
- [2] R. d. S. Ruiz, F. P. Amatte e K. J. B. Park, "Tornando Pública a Navegação "InPrivate"," em *Proceedings of the IcoFCS2012*, Brasília - Brazil, 2012, pp. 67-75.
- [3] T. Dienlin e S. Trepte, "Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors," *European Journal of Social Psychology*, 31 July 2014.
- [4] M. E. Delamaro, J. C. Maldonado e M. Jino, *Introdução ao Teste de Software*, 1 ed., vol. 1, Rio de Janeiro: Elsevier, 2007.
- [5] G. Aggarwal , E. Bursztein, C. Jackson e D. Boneh, "An Analysis of Private Browsing Modes in Modern Browsers," em *Proceedings The Advanced Computing Systems Association*, Washington, DC, 2010, pp. 6-6.
- [6] A. Mahendrakar, J. Irving e S. Patel, "Forensic Analysis of Private Browsing Mode in Popular Browsers," 25 April 2010. [Online]. Available: <http://mocktest.net/paper.pdf>. [Accessed at:30 November 2014].
- [7] H. Chivers, "Private browsing: A window of forensic

- opportunity,” *Digital Investigation*, vol. 11, n° 1, p. 20–29, 2014.
- [8] D. J. Ohana e N. Shashidhar, “Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions,” *EURASIP Journal on Information Security - Springer Open Journal*, 21 November 2013. [Online]. Available: <http://jis.eurasipjournals.com/content/2013/1/6>. [Accessed at: 03 December 2014].
- [9] E. Casey e G. J. Stellatos, “The Impact of Full Disk Encryption on Digital Forensics,” *ACM SIGOPS - Operating Systems Review (OSR)*, vol. Vol 42, n° Issue 3, pp. 93-98, 2008.
- [10] J. Oh , S. Lee e S. Lee , “Advanced evidence collection and analysis of web browser activity,” em *The Proceedings of the Eleventh Annual DFRWS Conference*, New Orleans - USA, 2011, pp. s62-s67.
- [11] Microsoft, “What is InPrivate Browsing?,” Microsoft, 15 November 2014. [Online]. Available: <http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing#1TC=windows-7>. [Accessed at: 15 November 2014].
- [12] Mozilla Contributors, “Private Browsing,” Mozilla, 15 November 2014. [Online]. Available: <https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info>. [Accessed at: 15 November 2014].
- [13] Google Inc., “Chrome,” Google Inc., 15 November 2014. [Online]. Available: <https://www.google.com.br/chrome/browser/desktop/index.html>. [Accessed at: 15 November 2014].
- [14] Apple Inc., “Defending your online privacy and security,” Apple Inc., 15 November 2014. [Online]. Available: <http://www.apple.com/safari/>. [Accessed at: 15 November 2014].
- [15] Oracle , “Oracle VM VirtualBox,” Oracle, 15 November 2014. [Online]. Available: <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>. [Accessed at: 15 November 2014].
- [16] Tor Project, “What is the Tor Browser?,” Tor Project, Inc., 15 November 2014. [Online]. Available: <https://www.torproject.org/projects/torbrowser.html.en>. [Accessed at: 15 November 2014].
- [17] VMware, “All Downloads,” VMware, 20 November 2014. [Online]. Available: <https://my.vmware.com/web/vmware/downloads>. [Accessed at: 20 November 2014].
- [18] Die.net, “strings(1) - Linux man page,” 10 may 2009. [Online]. Available: <http://linux.die.net/man/1/strings..> [Accessed at: 30 June 2012].
- [19] J. Kornblum, . K. Kendall e N. Mikus, “Foremost website,” 06 June 2002. [Online]. Available: <http://foremost.sourceforge.net/>. [Accessed at: 12 October 2012].
- [20] S. Lee , A. Savoldi, S. Lee e J. Lim, “Windows Pagefile Collection and Analysis for a Live Forensics Context,” em *Proceedings of Future Generation Communication and Networking (FGCN 2007)*, Jeju-Island, Korea, 2007, pp. 97-101.
- [21] G. G. Richard III e V. Roussev, “A Frugal, High Performance File Carver,” em *Proceedings of the 2005 Digital Forensic Research Workshop (DFRWS)*, New Orleans - USA, 2005, pp. 97-101.
- [22] C. Vaughan, “Xbox Security Issues and Forensic Recovery Methodology (Utilising Linux),” *Digit. Investigation*, vol. 1, n° 3, pp. 165 -172, September 2004.
- [23] G. Grispos, T. Storer e W. B. Glisson, “A comparison of forensic evidence recovery techniques for a windows mobile smart phone,” *Digital Investigation*, pp. 23-26, 20 July 2011.
- [24] T. Courrejou e S. L. Garfinkel, “A COMPARATIVE ANALYSIS OF FILE CARVING SOFTWARE,” 12 September 2011. [Online]. Available: <http://www.dtic.mil/dtic/tr/fulltext/u2/a550119.pdf>. [Accessed at: 20 November 2014].
- [25] B. Carrier, “Open Source Digital Forensics Tools: The Legal Argument,” 10 October 2002. [Online]. Available: http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf. [Accessed at: 25 November 2014], pp. 1-10.
- [26] X-Ways Software Technology AG, “WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor,” X-Ways Software Technology AG, 10 November 2014. [Online]. Available: <http://www.x-ways.net/winhex/>. [Accessed at: 10 November 2014].
- [27] Discovery Channel, “Discovery website,” Discovery Channel, 07 October 2012. [Online]. Available: <http://dsc.discovery.com>. [Accessed at: 07 October 2012].
- [28] History Channel, “History.com website,” History Channel, 10 September 2014. [Online]. Available: <http://www.history.com>. [Accessed at: 10 September 2014].

APOC@LYPSE: THE END OF ANTIVIRUS. WHEN THE ANTIVIRUS IS THE THREAT

By Rodrigo Ruiz, researcher at CTI Renato Archer and
Rogério Winter, Colonel at Brazilian Army

We present the proof of concept of a new cyber weapon that has the potential to paralyze an entire nation with irreversible damage, caused by nation state-sponsored attacks (Ministry of Justice of Georgia 2011) or terrorists. Apoc@lypse Technique removal of pages in the book '*Apoc@lypse: The End of Antivirus*' (Ruiz, et al., 2015) clearly demonstrates the fragility of our defences. We were taught for more than 30 years that in the digital age, we should trust our antivirus system and always keep it updated. You can control the antivirus market and turn it against your opponent, since to do so protects your family photos, even those that protect our trade, finance and military strategies. Undetectable, fast and devastating for the computer data hit.

INTRODUCTION

An anti attack can be related to the context of asymmetric conflict where the asymmetric actors have power(s) that differ significantly, divergent political and military objectives. With that in mind, they seek strategic advantage to counterbalance their own weaknesses, and compensate for the technological superiority of its opponent. The utilisation of a cyber weapon is one way to conduct a cyber attack. Anyone can learn about and create effective cyber weapons. For this, it is necessary a computer, Internet connection, the time and patience to learn about software, hardware, and network vulnerabilities.

The unpredictability of cyber attacks often creates cascading effects that were outside the original intentions of the attacker, effecting results that were not in the initial planning.

In his article, Clay Wilson (Wilson 2015) mentions the recent studies regarding cyber attacks, which revealed common features that describe a cyber weapon:

- a. A malware attack campaign can combine multiple malicious programs for espionage, data theft or sabotage.
- b. The stealth capability allows you to maintain the secrecy of the operation for a long period.
- c. The attacker has detailed knowledge about the operation of the target system.
- d. There is a special kind of computer code to bypass cybersecurity protection technologies.

Moreover, another striking and present characteristic of the cyber weapon is the possibility of the concepts reuse that are also part the cyber weapon. In the other words, a malware analysis can find a number of features that will be learned and will used in the counterattack. In contrast, a kinetic weapon will be certainly destroyed if a defect or fault occur during the launch. As well as, if a kinetic weapon is found in the battlefield a specialized military unit will destroy it.

Wilson's work (Wilson 2015) helps us to introduce the Apoc@lypse. The Apoc@lypse Technique was discovered in tests for verification of the effectiveness of antivirus¹ and its resilience in case of attack. The DOD (US Department of Defense 2010) developed the following concept of Mission Assurance:

"A process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the execution of DoD mission-essential functions in any operating environment or condition."

The concept of Mission Assurance involves not only military structures, but also adjusts itself perfectly in Business, Government and, Research and Development (R&D). In this context, the use of the antivirus has been emphasised as an information security dogma. In addition, it has been repeated as a best practice in almost all information security policies.

CYBER ATTACKS AND KINETIC ATTACKS

With the evolution of computing systems, many critical infrastructures (Command & Control, Air Traffic Management, Power Plants, Weapon Systems, etc.) use advanced automation making modern society technologically dependent. This dependence makes the Cyberspace a new way to conduct wars as in ground, air or sea combat.

A successful Israeli fighter aircraft attack to a suspicious nuclear plant in Eastern Syria sparked up the expert's curiosity about the failure of the Syrian radar system (Adee 2008). Supposedly, the Russian-built radar system was state-of-the-art to warn and it was not able to detect Israeli fighter aircraft invading the Syrian territory.

To protect cyberspace during a war, it is necessary to identify the main events in space and time, and to understand how Cyber Threats could

produce damage to critical infrastructure that are used for operations.

For now on, imagine a hypothetical situation where your enemy can be able to take control of the anti-aircraft missiles system avoiding your reaction. Now, think about a protection system that instead of protecting your territory destructs itself. Interestingly, it is possible and actually occurs in nature. We will explain how this phenomenon can occur in protecting a system, more specifically with an antivirus system.

An antivirus system has an important role in cyber defence, but an unfortunate finding was obtained after an analysis of the attacks carried out in recent years. Invariably, antivirus detection of errors is present in almost everyone. We have believed that our antivirus systems are capable to identify and fight against the cyber threats. Indeed, the reality is quite different. For instance, as it is mentioned in (Ministry of Justice of Georgia, 2011), the attack strategy against Georgian Government was to use Unknown Malicious Program that none Antivirus Products could identify the threat, by the time of discovery. In this case, the failure of malware detection contributed in decisive way for the success of the cyber attack.

As mentioned earlier, there is a possibility of a protection system to fail and destroys itself. If we establish a metaphor with the human body this situation is called autoimmune disease. Autoimmune disease is a disease in which a person's immune system wrongly attacks its own healthy tissues. In addition, immunological body systems attacks its own cells and tissues.

In our research, we identified some similarities between the human body and the cyber body thus; we tried to simulate certain conditions. Consequently, we managed to establish the first autoimmune cyber disease and thus the antivirus system is able to attack the computer system, which it is defending.

Apoc@lypse: The End of Antivirus (Ruiz, et al., 2015) clearly demonstrates the fragility of our defences. The Apocalypse Technique is a generic and extremely efficient way to bypass the protection of the

¹ In this paper, we will use antivirus and antimalware interchangeably because antivirus is a well-known word.

antivirus system. The technique explores undisclosed vulnerability of the system's antivirus and allows infection in the furtive form a machine target and to destroy the operating system and stored data. We implemented the Apocalypse Technique in software and it can choose among several existent forms of infection. The signatures concept has been "copy and pasting" since the first antivirus, but it has an error inside the protection concept.

THE CYBER WEAPON

We present the proof of concept of a new cyber weapon with the potential to paralyze many information systems and different operational systems causing damage irreversible form. In this paper, we considered the following definition of the cyber weapon:

"a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings". (Lasiello 2015).

The cyber weapon can be classified by type: physical and logical weapon. Physical weapons are malicious artifacts found in the hardware of a computer or other devices under the management of a computerized system. More recently, this type of cyber weapon has received greater attention because of the great difficulty of detection.

"Cyberwarfare analysts argue that while most computer security efforts have until now been focused on software, tampering with hardware circuitry may ultimately be an equally dangerous threat". (Markoff 2009).

On the other hand, the logical weapon is a cyber weapon crafted from a failure or an error in a software, which puts it in a vulnerable situation, allowing cyber exploitation. More accurately, the Apoc@lypse Technique exploits a vulnerability in the concept of misuse detection in the antivirus system. The misuse

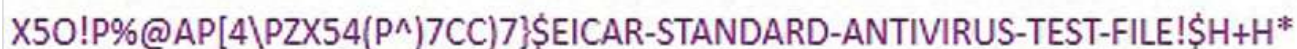
detection is a fundamental concept of all antivirus systems, from the earliest to the current ones.

In an antivirus system, we have two different approaches: misuse detections and anomaly detection. Misuse detection is based on signatures or patterns of attacks to the computational system. Some actions directed at the objects of the system are considered as threatening, such as file deletion, hard disk formatting or attempts to modify privileged access files. Well-defined and known actions to the weak points of a system form the signature of the attacks. The detection of attacks happens by observing such actions occurring with specific objects. Conversely, anomaly detection is based on the definition of the expected behaviour of a host computer or its network. Therefore, a profile of the normal behaviour is captured using statistical methods and association rules, for example; and the detection of attacks then takes place by spotting actions that were unexpected according to the profile.

The Apoc@lypse Technique is based on injection of any DNA fragment of virus (Figure 1) in benign files, without necessarily interfering with the functionality of these files. Depending on chosen virus DNA some antiviruses will be affected and others not because antivirus companies have different methods of handling viruses. However, a special DNA affects all. In fact, the technique is very simple to be implemented with the use of a string similar to the EICAR, the Anti-Malware Test file.

In the first place, EICAR stands for European Institute for Computer Antivirus Research. They defined a test file, which it has been provided as the "EICAR Standard Anti-Virus Test File" (Figure 1). According to the EICAR, this string is safe to pass around because it is not a virus and does not include any fragments of viral code.

For instance, imagine the calculator on your Windows operating system™ receiving pieces of virus within the same executable file. From this standpoint, we have a calculator marked for death.



X5O!P%#@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

Figure 1: The Anti-Malware Test file (source <http://www.eicar.org/86-0-Intended-use.html>).

This piece of virus that we introduced in the calculator is harmless and does not represent any risk to the system. We deployed the Apoc@lypse technique in 150 different antivirus brands and after the process of injection, all products began to identify the executable file of the calculator a great and terrible threat. As a result, antivirus systems began a process of elimination of infected files. In this case, the enemy is not the DNA fragment of the malware, but the antivirus system that attacks all inject files. This concept now presented, is a trigger for the start of a large-scale phenomenon, which we call Cyber Autoimmune Disease.

A very important aspect in this type of operation is a secrecy. In this case, camouflage techniques are more indicated to obtain total operation secrecy and facilitate access to the target. With the Apoc@lypse Technique, it is possible bypass with great success the antivirus protection and create a prototype of the Cyber Weapon. We use the concept of the transporter of malware DNA in the cloaked form.

This transporter, metaphorically, is called "bacterium". Many bacteria live in the human body symbiotically and are recognised as beneficial to our body, such as the Lactobacilli. Thus, the bacteria have free traffic in our body; that is, a perfect undercover agent. Our prototype allows the programming of the bacteria to locate target files and inoculate the DNA of the malware beyond other tasks, such as data exfiltration, espionage, data theft, or sabotage.

The bacterium concept is taught in biology in primary education, but it is extremely effective when combined with a computer game, such as the old Tetris². In Figure 2, we present the technical step-by-step of Apoc@lypse that is able to destroy the computer system.

FINANCIAL IMPACT ON THE CORPORATE WORLD

The assessment of the economic impact is an open question in cyberspace. Specialised reports of security companies point to an adverse scenario where certainty of the attack itself is accompanied by unpredictability of

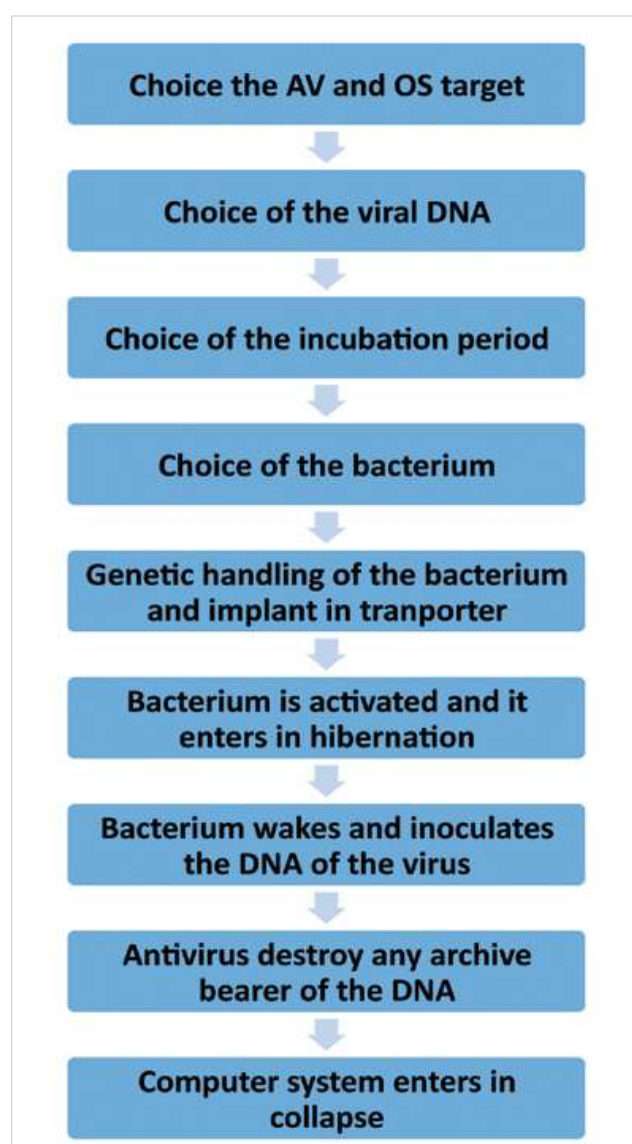


Figure 2: Apoc@lypse Technique - cyber weapon step-by-step.

the day and place of the cyber attack.

The reports carried out by the security companies often present economic impacts in the several economic sectors. However, the fact is that each new report of security invariably we can identify a binding with a marketing campaign to launch new products and services of that company.

There are several discussions about how to assess the economic loss caused by a cyber attack. However, this assessment depends on two key factors: first, the companies need to know the size of the loss

2 <http://www.download3k.com/Install-Tetris.html>

and secondly, they need to disclose that information. Therefore, the key problem with this finding is that the companies need to develop a situational awareness about what really was affected by the attack.

When we visualise cyberspace, four information assets are mandatory to consider in terms of mitigating risks and planning the defence: technology, people, processes and environment. In this way, we need to consider them when we estimate the economic impact before, during and after a cyber-attack. The ability to measure the damage caused by a cyber attack allows us to invest with great efficiency in cybersecurity.

Prior to 2010, the largest information security concern was with the theft of banking information. However, in 2010 a successful cyber attack established a change of thought in information security. We are referring to the Stuxnet. Stuxnet is a malware that was used for the first large-scale attack on SCADA systems, in Iran. A cyber event so sophisticated that it was able to break the pillars of cyber security: technology, people, processes and environment. With a very complex code, the Stuxnet, used 04 zero-days, and explored technological resources. This cyber attack resulted in the theory of a new weapon constructed by secret services to damage the Iranian nuclear program. We can imagine the economic impact in the Iran nuclear program.

The economic issue is important to society, not least because several wars were initiated by economic disagreements. It seems that everyone wants to have some value to use for many different purposes. The press show us amazing news, some vendors use Fear, Uncertainty, and Doubt, and to compare to other infections. The following lists the most emblematic attacks of the virus/malware that caused the greatest economic damage:

- a. Chernobyl -CIH (1988) between \$20 million and \$ 80 million; in addition, it destroyed data.
- b. Melissa (1999) caused damage estimated at 1 billion euros.
- c. ILOVEYOU (2000) the estimate of the financial damage caused was between \$10 billion and \$15 billion.
- d. Code Red (2001) estimates a million infected computers, and damages of \$ 2.6 billion.
- e. SQL Slammer (2003) infected 75.000 computers in 10 minutes and messed up the online traffic.
- f. BLASTER (2003) the estimated damage was between \$2 billion and \$10 billion.
- g. Sobig. F (2003) the estimated damage was between \$ 5 to \$ 10 billion, with more than a million infected PCs.
- h. Bagle (2004) the estimated damage was at tens of millions of dollars.
- i. Mydoom (2004) decreased by 10% global Internet performance and increased the loading time of 50% sites.
- j. Sasser (2004) Sasser caused tens of millions of dollars in damage.
- k. Conficker (2009) The Cyber Secure Institute estimated the economic loss due to the Conficker worm could be as high as \$9.1 billion. According to Conficker Working Group, this was 35 Million unique IP's.

Malware detection systems are gradually becoming objects of criticism from security experts, in particular in terms of detection rate. The criticisms are directed to use the old technology-based signature approach to fighting recent threats. Currently, several specialized publications realizing efficiency tests on anti-malware systems. The results are very encouraging, but they do not match the reality of current threats. Maybe the blind spot in the process is the methodology employed, which does not allow a complete understanding of how the various anti-malwares are tested. In 2012, Brazilian scientists from the Center for Information Technology Renato Archer (Brazil) have applied the Brazil Method of Anti-malware Test (Filho, et al., 2014) for anti-malware systems sold on the Brazilian market. The result obtained was a detection rate different from those informed by magazines and specialised consultancies around the world. The tests were focused on the Brazilian internet domain and the average detection was only 50%.

For nearly four decades, since the invention of the first antivirus, we thought that were safe; but in fact, in each new virus or malware we are surprised at the

time to defend ourselves. Cybersecurity depends on reliable operation of an infrastructure, which by its nature is critical.

HOW SHOULD WE DEFEND OURSELVES?

How does to defend yourself from an enemy that has this type of cyber weapon? An engineer from a big antivirus company, who declined to identify himself, wrote:

“Inserting parts of viruses in benign files is quite ingenious and I recognise the failure of all AV engines... It’s a structural behaviour and probably impossible to ignore with the current architecture.”

The rhetorical question to the problem: what is the solution? The answer is easier said than done. In cybersecurity, technology, environment, people, and process are inseparable. We believe that the time has come to have in hands a pen and a blank piece of paper, and rewrite every line of code again. In other words, structure the defence with a vision to fight against the recent threats.

CONCLUSION

Archimedes³ used to say, in the Doric speech of Syracuse: “Give me a place to stand and with a lever I will move the whole world.” The current paradigm is a computer and an internet access point to change the history of the world.

Security is a feeling of protection; necessary and indispensable to a society and each of its members, against threats of any kind. Defence is the capable action to sustain security feeling (Escola Superior de Guerra 2013). Many current systems are designed based on are past knowledge and concepts, but economic issues have not been updated. In 1987, Denning wrote:

“... on existing systems with known flaws are not easily replaced by systems that are more secure-mainly because the systems have attractive features that are missing in the more-

secure systems, or else they cannot be replaced for economic reasons (Denning 1987)”.

The technologies that we trust to provide protection against cyber threats must be adapted to the context, in which they are used, as well as processes, people, environment of usage. In this context, the weapon that defends is the same that destroys the system. All information security standards insist that a best practice includes an installed and updated antivirus. The current time is the cybersecurity and the computation is ubiquitous in people’s lives. According to (Ford 2004):

“While the antivirus industry has been steadily improving over the years, some might be surprised to learn that the fundamental technology used for detecting and removing viruses has changed very little over time.”

It is amazing that after a decade of Ford’s statement, we can demonstrate that the technology has changed very little in combating existing cyber threats. The Apoc@lypse Technique is a proof of concept. Besides the discrete evolution, a serious flaw in the detection system allows it to be exploited as a cyber weapon.

We can demonstrate that is possible to take control of an anti-malware system and to command operating system destruction. The Apocalypse Technique proof of concept is more effective in Windows Operational System, but for the other operational systems (Linux, Android, UNIX e Mac) the effects can be less catastrophic.

The Apocalypse Technique explores undisclosed vulnerability in the anti-malware systems. Technical efficiency of Apocalypse was successfully tested in 150 anti-malware system existing in the international market. The Apoc@lypse Technique is undetectable, fast and devastating for the computer data.

The big question is that all nations defend themselves with the same vulnerable systems. This vulnerability can be used to attack the enemy with a similar system that can protect it.

How does the antivirus industry see this situation?

3 <http://www.math.nyu.edu/~corres/Archimedes/Lever/LeverQuotes.html>

- a. Denial: It is extremely difficult for the industry to admit the problem publicly.
- b. Affliction: The antivirus companies do not know how to solve the problem.
- c. Laziness and Money: For security software, the complete solution of cyber problems represents the need to find another product to sell.

What will you do? ■

REFERENCES

- Adee, Sally. "The Hunt for the Kill Switch." IEEE Spectrum. May 01, 2008. <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch> (accessed November 30, 2015).
- Denning, Dorothy E. "An Intrusion-Detection Model." TRANSACTIONS ON SOFTWARE ENGINEERING. Piscataway, NJ, USA: IEEE Press, 1987. 222-232.
- Escola Superior de Guerra. "CAMPOS DE ATUAÇÃO DO PODER NACIONAL." In Manual Básico da Escola Superior de Guerra - Elementos Fundamentais Volume I, 66 - 84. Rio de Janeiro: Biblioteca General Cordeiro de Farias, 2013.
- Filho, Antonio Montes, Rogerio Winter, Rodrigo Ruiz, Fernando Pompeo Amatte, José Geremonte Garcia, and Bruna Stefani de Oliveira Martins. "Brazil Method Anti-malware Test and the Implications For Cyber Defense." XVI Symposium of Operational Applications in Areas of Defense (SIGE). São José do Campos - Brazil: Aeronautics Institute of Technology - ITA, 2014.
- Ford, Richard. "The future of virus detection." Information Security Technical Report Vol. 9, No. 2, 2004: 19 - 26.
- Lasiello, Emilio. "Are Cyber Weapons Effective Military Tools?" Military and Strategic Affairs, 2015: 23-40.
- Markoff, John. "Old Trick Threatens the Newest Weapons." The New York Times. October 26, 2009. <http://www.nytimes.com/2009/10/27/science/27trojan.html> (accessed November 30, 2015).
- Ministry of Justice of Georgia. "CYBER ESPIONAGE - Against Georgian Government (Georbot Botnet)." Data Exchange Agency. March 2011. <http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf> (accessed December 11, 2015).
- Ruiz, Rodrigo, Rogerio Winter, Kil Park, and Fernando Amatte. Apoc@lypse: The End of Antivirus. Charleston: Amazon, 2015.
- US Department of Defense. "DoD Policy and Responsibilities for Critical Infrastructure." Federation of American Scientists. January 14, 2010. http://fas.org/irp/doddir/dod/d3020_40.pdf (accessed December 06, 2015).

Wilson, Clay. "Cyber weapons: 4 defining characteristics." GCN. June 04, 2015. <https://gcn.com/articles/2015/06/04/cyber-weapon.aspx> (accessed December 06, 2015).

Zan, Tommaso De, Fabrizio d'Amore, and Federica Di Camillo. "Protezione del traffico aereo civile dalla minaccia cibernetica." Istituto Affari Internazionali (IAI). December 09, 2015. <http://www.iai.it/it/pubblicazioni/protezione-deltrafficoaereo-civile-dalla-minaccia-cibernetica> (accessed December 13, 2015).

ABOUT THE AUTHORS



Rodrigo Ruiz is researcher of CTI – Information Technology Center - Renato Archer, Campinas, Brazil. He is also a member of the SDIWC (The Society of Digital Information and Wireless Communications) and co-author of the book "*Apoc@lypse: The End of Antivirus*" and many papers about privacy and security (https://www.researchgate.net/profile/Rodrigo_Ruiz3). Email: rodrigoruiz@outlook.com



Rogério Winter is Colonel in the Brazilian army with more than 25 years experience in military operations and information security. He received the Master's degree in Electronic Engineering and Computation by Aeronautics Technological Institute-ITA and is a member of the SDIWC (The Society of Digital Information and Wireless Communications). Today, he is dedicated to cyber warfare, command and control, and decision-making process and coauthor of the book "*Apoc@lypse: The End of Antivirus*". Email: rogwinter@gmail.com

ACKNOWLEDGEMENT

We would like to express our thanks to the Fábio Renato Winter for his review work and to Victoria Ganzert for creating the name and publishing the Apoc@lypse.

CYBER SECURITY REVIEW

Unique content | Global reach | In print and online



www.cybersecurity-review.com



Subscribe at:
www.cybersecurity-review.com/subscribe

CORROSIVE SECRECY AND CONFIDENCE: THE PARADOX AMONG BYPASSING CRYPTOGRAPHIC SOFTWARE, LOSS OF PRIVACY AND INFORMATION SECURITY

By Rogério Winter, Brazilian Army – Cyber Defense and
Rodrigo Ruiz, Center for Information Technology Renato Archer (CTI)

The security of information has grown in importance worldwide. When businesspersons travel, they transport sensitive company data among offices, cities and even countries. It is noteworthy that many mobile devices are stolen each year and with that, information confidentiality of company's strategic information confidential can be compromised. Our work has evolved to an analysis of two existing consecrated encryption systems on the market: Bitlocker (Microsoft) and Bit Defender Total Encryption 2015 (Bitdefender). We were able to prove that outdated concepts are still being used to protect the information and guarantee the privacy. We show how failures in their development, commercial inconsistencies and poor implementation can compromise the privacy and information security.

Keywords: Encryption, Confidentiality, Data security, Forensics, Privacy, BitLocker, BitDefender.

INTRODUCTION

We introduce this paper with a citation from the Holy Bible, Luke 8:17 ^[1] *"For there is nothing hidden that will not be disclosed, and nothing concealed that will not be known or brought out into the open"*. The scientific findings reported in this article do not focus on religious subjects, but a proper truth to the current environment of information security.

In this article, we find security flaws in renowned encryption systems in the international market – Bitlocker (Microsoft) and Bit Defender Total Encryption 2015 (Bitdefender). We were able to prove that outdated concepts are still being used to protect the information of people, companies and governments.

Cryptography is not the only means of providing information security, but rather one set of techniques."^[2]

The cryptographic algorithms are developed over a mathematical foundation that proves the correctness

of such algorithms based on how much computational power would be needed in order to break them. In other words, the attack on effective cryptographic algorithms requires a large time consumption of computers, rather than trivial techniques, to be effective.

All things considered, an attack on such system is virtually impossible or uneconomical.

However, cryptographic algorithms are implemented in software products designed to facilitate the use of single users or corporations. Unquestionably, therefore, the problem is not in the algorithm but in how it is used in the software. Using outdated libraries and software implementation errors ends up weakening the protection of the information. Let us remember that a chain is only as strong as its weakest link.

The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and

critical errors that can lead to serious vulnerabilities in software ^[3]. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. We can classify errors in this way: Insecure Interaction between Components, Risky Resource Management and Porous Defences. In this paper, we focus on two errors: Incorrect Authorisation and Authorisation Bypass Through User-Controlled Key - CWE 639 ^[4].

In this context, we will discuss the security process, because it goes beyond the specific use of the encryption algorithm. Security is wide and should be considered in a systemic view, with all the details involved.

This work is built over the hypothetical answer to the following question: Is the Hard Disk Encryption software effective under the proposed test circumstances?

FINANCIAL IMPACT ON THE CORPORATE AND MILITARY WORLD

Nowadays, the choice of professionals who provide technical support to a large portion of politicians, businesspersons and in the military area is one of the great challenges in information security management.

Therefore, the best-qualified person is rarely the leading technical support. Instead, IT crew is frequently selected by the criterion of confidence. Such behaviour has the potential to create security holes that can be exploited by criminals and competitors. Nevertheless, technical disability and unethical behaviour are also causes of data security breaches.

The risk of infiltration by criminal elements in business and in their own governments makes the population vulnerable to manipulation and loss of confidential data.

Both businesses and governments are subject to such infiltration. Criminal organisations are allocating their representatives in strategic positions for the purpose of illicitly obtaining precious inside information. Criminals go so far as to sponsor people in their studies to fulfil this goal ^{[5] [6]}.

A Brazilian oil company reported that the theft of equipment containing sensitive information about the

discovery of new oil wells affected the value of its shares negotiated on the stock market ^[7].

A survey by the Ponemon Institute presents interesting and alarming data on the damage caused to businesses, where the theft of a laptop can cost up to \$115,000 in strategic information loss. The same survey shows that the encryption significantly reduces the cost of the theft while the theft of a machine with unencrypted HD costs U.S. \$56,165; one that is encrypted presents the loss of U.S. \$37,443 ^[8].

A report in ComputerWorld magazine's website has attracted attention by bringing up actual cases of IT professionals very well placed in large and reputable companies, using their positions of trust to commit crimes. This report also presents research, which suggests that one in three IT professionals spy systems of the company and his colleagues accesses data such as contracts, wages, emails, and other strategic information ^[9].

The various stories about theft and loss of computers outline a target profile attack where the victim (person or business) are part of campaigns obtaining vital information to feed some business strategy.

Several Hard Disk Encryption solutions can reduce the impact of the executive computer theft. When a company security policy considers the adoption of Hard Disk Encryption, they implicitly place trust in the reputation of the supplier of the safety solution and the robustness of the encryption solution adopted.

CONTEXT

Cryptanalysis is the study of the procedures necessary to attempt to compromise the cryptographic techniques, and, more generally, the security services of information ^[10]. Thus, cryptanalysis is the art of trying to figure out the ciphertext and/or the logic used in their encryption. Encryption solutions use very complex algorithms, such as: AES, Serpent and Twofish, etc.

However, the cryptanalysis process is based on the search of patterns in the encrypted data. Indeed, when a computer is analysed by forensic perspective, the data recorded on hard disk are used to assemble the image files.

This work proves that in some circumstances, with simple information and little time available, it is possible to extract the clear text from the encrypted content. This is because during the implementation of the security solution, some errors give hints of methods, keys and ciphers used to encrypt messages.

RELATED WORK

On the discussion of Block Ciphers,^[11] classifies the possible attacks attempts based on the data that an attacker can procure:

Ciphertext-only attack, where an attacker has access only to ciphered information. He knows of plaintext attack, where an attacker has access to plaintext messages and its ciphered counterparts. Chosen plaintext attack is where the attacker chooses a specific set of plaintext messages and is able to acquire its ciphered counterparts. Adaptively chosen plaintext attack is where an attacker chooses the plaintext messages based on the cipher result of the previously chosen plaintext message. Chosen ciphertext attacks are where an attacker chooses different ciphered messages and is able to acquire its deciphered counterparts. Furthermore,^[12] divides possible attacks into two categories: First, practical attacks, that focus on implementation and usage issues; second, theoretical attacks, that focus on the mathematical aspects of the chosen cipher algorithms. However, this attack has a practical character. Proposing a methodology to evaluate a given system security,^[12] presents the attack tree, a structure that describes a system security using different attack possibilities as parameters. It also gives an example attack tree on the PGP email security software. As the author indicates, the previous tree attack can easily be extended to include more attack formats.

Although the tree is based on PGP, it could easily fit another software. Besides that, in the previous example, one possible inclusion under item 1 of the tree could be item 1.3 – “Exploit software implementation weakness”. This kind of attack would, through the active exploitation of software design issues or vulnerabilities, lead to full message decryption. Under^[11] and^[12] classification system, proposed

attack 1.3 would be a ciphertext-only and practical instead of theoretical. This paper methodology is based on this attack type.

ABOUT ENCRYPTION SOFTWARE

The OPSWAT^[13] report, in September 2011, about Hard Disk Encryption Market Share, indicates that the market was divided among Microsoft (92.94%) and other manufacturers (7.6%) (Figure 1). In addition to the market division, there are other manufacturers involved, as shown in Figure 2. In this article, we will focus on Microsoft and BitDefender due to the software user’s preferences, among those, which are available on the market (Table 1).

Software	Developer
BitLocker	Microsoft
Bit Defender Total Encryption 2015	Bitdefender

Table 1: Tested software.

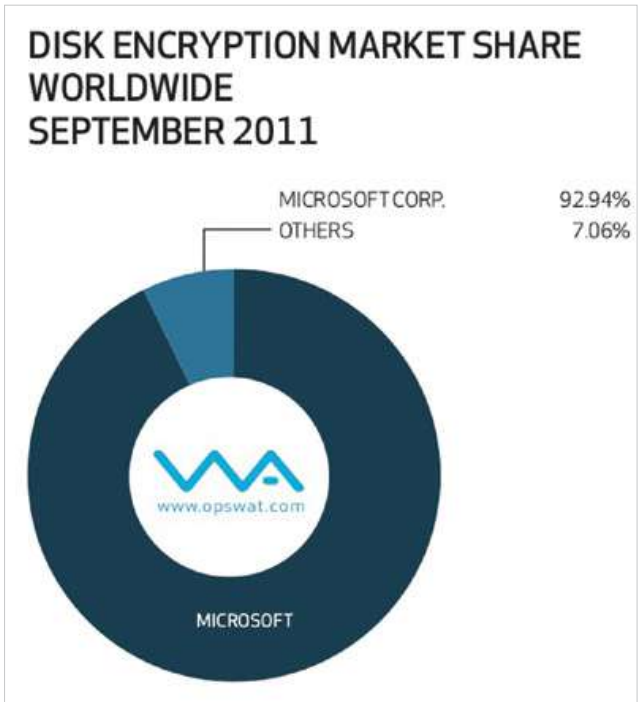


Figure 1: Disk Encryption Market Share Worldwide. Source: OPSWAT Report.

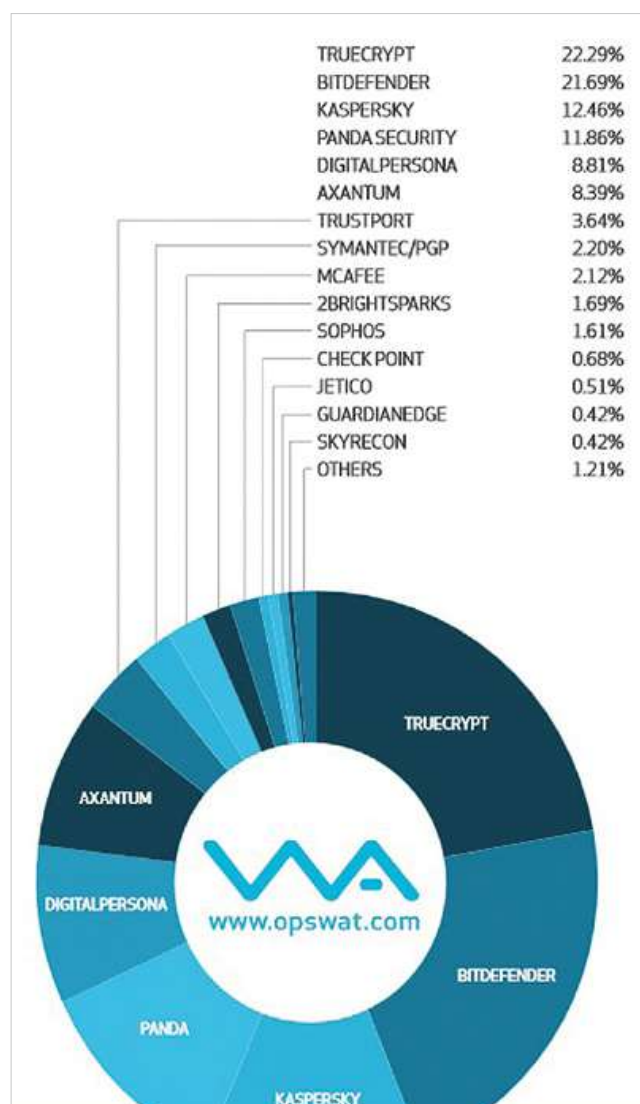


Figure 2: Hard Disk Encryption Market share.
Source: OPSWAT Report.

Bitlocker

According to the Microsoft website, BitLocker was enhanced for Windows 7 and is available in the Ultimate and Enterprise editions. BitLocker protects documents and passwords by encrypting the entire Windows drive on where your data is. When BitLocker is enabled and any file saved on drive is encrypted automatically.

BitLocker To Go is a new feature in Windows 7, which allows blocking of portable storage devices easily left in the wrong places, such as USB flash drives and external hard drives.

Bit Defender Total Encryption 2015

Bitdefender antivirus software is a suite developed by Romania-based software company Softwin. Bitdefender has a software component for encryption of files and folders called BitDefender Total Encryption 2015. The file encryption function is responsible, according to the manufacturer, to create a secure and encrypted environment.

The system provides the user with an encrypted virtual drive, which is the logical representation of a file extension BVD (BitDefender Virtual Drive) as shown in Figure 3.

The basic structure of a BVD file consists of two segments, namely: data and footer. The data segment stores the encrypted user data while the footer holds records needed to validate the file and protection of SALT.

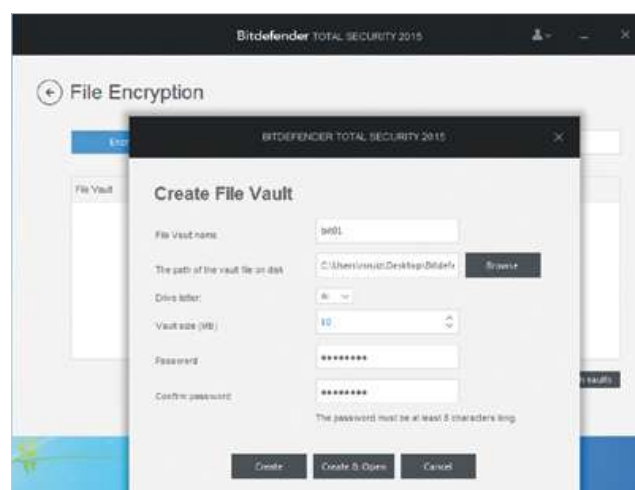


Figure 3: Bit Defender Total Encryption.
Source: Bit Defender Software.

METHODOLOGY R2K AND MATERIALS FOR THE TEST

According to Galliano^[14], method is the “set of steps, neatly arranged, to be overcome in the search for truth, in the study of a science or to achieve a particular purpose”.

Software testing is the process of verifying that the product complies with certain specifications and that it works properly for the function it was designed to fulfil. Denning^[15] observes that the major part of existing systems have vulnerabilities which make

them susceptible to attacks, invasions and other kinds of abuse; moreover, the maintenance to avoid all such deficiencies is not viable technically nor economically.

The goal of software testing is to show the presence of defects if they exist^[16]. Likewise, the goal of R2K test method is to identify possible weaknesses in the cryptographic systems that undermine the availability, integrity, confidentiality and authenticity of the information.

The method used in the tests can be applied generally and consists of four stages presented in Figure 4: research, test, test result and dissemination.

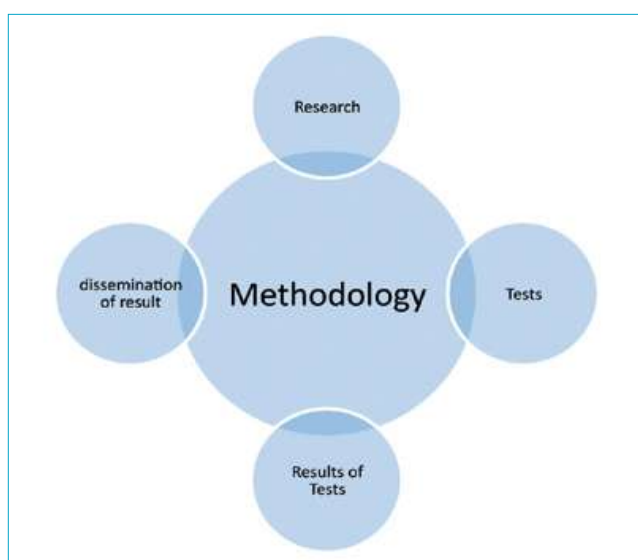


Figure 4: Methodology R2K.

Research – we study documentation to analyse the operation of software and usage guidance, promises of its manufacturers and finally the security solution files. Although they have the same goal, each software uses technology and distinct methods.

Software implementations can expose encryption break possibilities for various reasons, such as errors in development, failure in mathematical interpretation of the algorithms, disability in file structures, headers, backups, compromised passwords and mistakes over the management guidelines.

Test – for the tests performed, we used the following tools and software. A notebook equipped with Intel® Pentium® Dual Core with 3.0 GB of memory.

When testing a security feature, it is necessary to define the functional requirements of the same, and the profile of the attacker that will try to disable or override this feature.

In this article, we start from the methodological framework presented by^[17] for the construction of the following methodological model.

The profile of the attacker assumes that it has access to the user's BitLocker and BitDefender container at two different times. When it was first created and after the user stored valuable information on it and changed its password.

The hypothesis to be tested emerged from the analysis of the hex code of a file created by BitLocker and BitDefender the comparison of the hex code of the same file after executing the procedure to change the user's password to access the container. The software tools used to study the software behaviour BitLocker and BitDefender are available as low-cost or free software.

BitLocker Test

We created four virtual drives and sent them to BitLocker users, along with the original password. We asked volunteers to add personal information, change the password and then send us back the virtual drive.

In the tests performed, we found that no matter how many times the user modified the container password protected by BitLocker, the recovery key was always the same as presented in Figure 5. With the recovery key, it was possible to open all virtual drives and access all the information added by the users.

With the use of a recovery key, which is a second password available to open the encrypted data, the manufacturer reduces the security of their system, increasing the attack surface and the chances of a possible opponent achieving success during an attack. Unquestionably, on a recovery key composed by 48-digit (0-9), the combinatorial possibilities of give a large space of distinct valid recovery keys, but it is clearly much lower than the one given by the password, which can be built with 100 characters including all characters of the ASCII table.

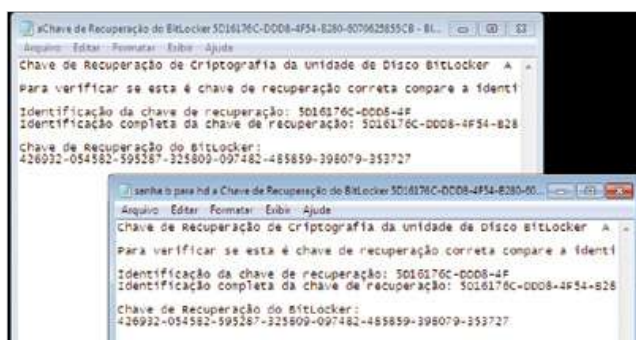


Figure 5: BitLocker key recovery.

BitDefender Test

We have created a BVD file named Bit01.bvd with password 123456789. Then a copy of the file was performed (Figure 6), named Bit02.bvd. The file had its password changed to 987654321. We enabled the virtual drive and added text file with sensitive information in Bit02.bvd. After those initial procedures, in theory, we have two files with different passwords and content.

We then applied the following technique in Bit02.bvd file. We merged the known password Bit01.bvd with data session Bit02.bvd file resulting in a third Bit01_Frankenstein.bvd file. In Figure 8 we can see the stretch of 2 BVD files passwords where one was mixed with each other to create a third file containing a password known Bit01.bvd (123456789) and encrypted data from Bit02.bvd. As a result, it was possible to open the contents of Bit02.bvd with password stored in Bit01.bvd (Figure 8).

With this simple technical procedure, the owner of any later release of Bit02.bvd file and the password used in the creation of Bit01.bvd will have access to the encrypted file content. The vulnerability found is similar to that reported in the article “Security Issue on Cloned TrueCrypt Containers and Backup Headers”^[21]. Although the article emphasized the TrueCrypt problem, we explored the vulnerability of Bitdefender the same way.

RESULTS AND DISCUSSION

In the present study, it was possible to identify the weakness of software Hard Disk Encryption BitLocker and BitDefender. The software has been selected among those present in the market and preferred by



Figure 6: Backup file Bit01.bvd

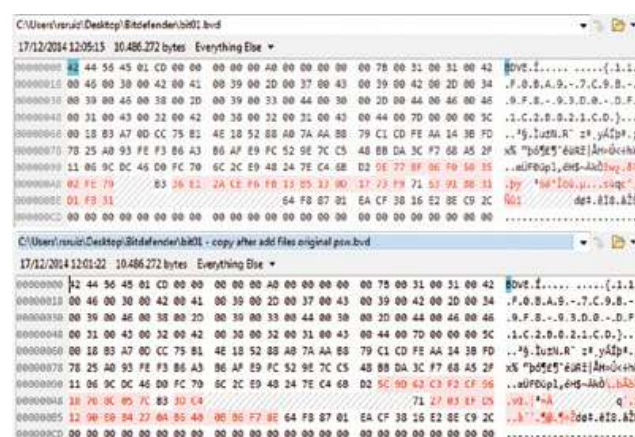


Figure 7: Password in file BVD.



Figure 8: Opened files.

users who are more concerned with security. After the tests performed with the software tools we can return to our premise at the beginning of the paper: Is the Hard Disk Encryption software effective under the proposed test circumstances? The answer is NO.

Businesspersons often move around the offices, cities and even countries. It is a well-known fact that airports, railway stations and subway stations are places where bags containing notebooks, smartphones and other electronic devices are often lost or stolen. The loss or theft both intentional and accidental create opportunities for sensitive data of one company to be disclosed. With proper techniques, as reported in this paper, the disclosure of information is almost inevitable.

Many companies concerned with data security adopt cryptographic solutions, such as BitLocker and BitDefender. Indeed, the adoption of security solutions is deeply influenced by a good marketing campaign and the suitability that the developer has in the market. Obscurity in the implementation of security software just weakens the entire information security management. Another aspect to be considered is file sharing on projects that can neglect safety principles of information in the companies.

In the information security world there are “Ten Immutable Laws of Security”^[18], which are an interesting reference for the discussion, because they can be used in the composition of a security policy to mitigate risks in the information tract:

“Law #1: If a bad guy can persuade you to run his program on your computer, it’s not solely your computer anymore;

Law #2: If a bad guy can alter the operating system on your computer, it’s not your computer anymore;

Law #3: If a bad guy has unrestricted physical access to your computer, it’s not your computer anymore;

Law #4: If you allow a bad guy to run active content in your website, it’s not your website anymore;

Law #5: Weak passwords trump strong security;

Law #6: A computer is only as secure as the administrator is trustworthy;

Law #7: Encrypted data is only as secure as its decryption key;

Law #8: An out-of-date antimalware scanner is only marginally better than no scanner at all;

Law #9: Absolute anonymity is not practically achievable, online or offline.

Law #10: Technology is not a panacea.”^[17]

In our study, a dangerous paradox emerges between what is promised by the companies and the failure found in BitLocker (Microsoft) and Defender Total Encryption 2015 (BitDefender). Marketing campaigns to both softwares gives an image of total security, but the reality is somewhat different.

When dealing with information security, two concepts are evident: security and usability. Quantities are inversely proportional; the higher the security requirement, the lower the ease of use. According to the CWE/SANS Top 25 Most Dangerous Programming Errors^[3], in particular Missing Encryption of Sensitive Data, we identify an attacker to seek unorthodox ways to achieve success in their purposes. Often, the systems are equipped with usability requirements to earn the preference of users, but the impact of these requirements is not adequately addressed from the perspective of security.

In BitLocker’s case, one problem arises from the weakening of the security system with a weaker recovery password that is always the same regardless of the change of the container’s password. This is paradoxical to Law #7, because a weakened password gives a higher probability of success to an attacker. Moreover, we can observe another time when the Law #5 was broken, because developers intentionally create a much weaker recovery key. As we mentioned earlier, a chain is only as strong as its weakest link. The same situation occurred on Security weaknesses LM hash^[19], when the weakening password enabled attacks with great effectiveness. With a fragile protection, an attack using specific techniques to the container becomes a more viable step. A report from BusinessWeek in January 2011 depicts among other information that about 30% of help desk calls refer to resetting passwords^[20].

The situation of Bit Defender Total Encryption 2015 is a different. The use of misconceptions affects the security of the customer’s information. We merged

two encrypted containers and were able to open the resulting container with the password used in its creation. This is possible because when we create a container, the original password acts as a master key for all other versions of containers regardless of the password change. In addition, the software allows merging of different parts without checking the integrity of the container. The vulnerability is transmitted to all containers weakening the system and compromising the cyber security and the privacy of information.

CONCLUSION

We present facts in this article that clearly show the encryption software is deployed insecurely. There are important differences between the information presented during the process of sale and security of product in relation to what the user will actually receive. Independently, free software or paid software all presented similar problems. The management of identities and passwords is not secure. Microsoft created its "Ten Immutable Laws of Security" in order to make users aware of the need to take care of information security. Nevertheless, are they being applied to their security software?

As mentioned early, in "Security Issue on Cloned TrueCrypt Containers and Backup Headers"^[21] researchers have presented a different and little explored approach to access information inside containers encrypted through the usage of Truecrypt software.

Strangely, the TrueCrypt developers abandoned the project and among many other existing products, they advised its members to use BitLocker. However, we emphasize two interesting issues. The first, the legacy of truecrypt continues influencing directly others software project, as Bitdefender. Bitdefender allow the manipulation of headers to perform the password bypass as shown in this research. Secondly, the advice to use Bitlocker there is also no guarantee that all information will be security. Because, there is an immutable master key (recovery key) over the life of each Bitlocker partition.

The information security vision must be systemic, because cybercrimes try to take advantage of

operating system and protection systems failures. Security flaws can cause distrust and financial losses for both users as well as companies. Clearly, we can see that an old flaw is still present. In a world where a great competitive disadvantage can bring a harmful result for a company and depending on the degree of exposure can lead to business bankruptcy. Nowadays, the protection of information is vital for a companies, government, armed forces and people. Any failure of products must be properly addressed, regardless of implementation, deployment and management of security components. ■

BIBLIOGRAPHY

- [1] "Holy Bible, New International Version," 1993. [Online]. Available: <https://www.biblegateway.com/passage/?search=Luke+8%3A17&version=NIV>. [Accessed 26 December 2014].
- [2] A. J. Menezes, . P. C. v. Oorschot and S. A. Vanstone , "Chapter 1 Overview of Cryptography," in Handbook of Applied Cryptography, London - England, CRC Press, Inc., 1996, pp. 1 - 48.
- [3] S. Christey, "CWE/SANS Top 25 Most Dangerous Software Errors," 13 September 2011. [Online]. Available: <http://cwe.mitre.org/top25/>. [Accessed 20 December 2014].
- [4] The MITRE Corporation, "Common Weakness Enumeration," 30 July July. [Online]. Available: <http://cwe.mitre.org/data/definitions/639.html>. [Accessed 23 January 2015].
- [5] D. F. S. Cunha, "Criminalidade Organizada: antigos padrões, novos agentes e tecnologias," [Online]. Available: <http://www.pontourbe.net/edicao8-cirkula/186-criminalidade-organizada-antigos-padroes-novos-agentes-e-tecnologias>. [Accessed 21 February 2014].
- [6] Instituto Marconi, "Como funciona o PCC - Primeiro Comando da Capital," [Online]. Available: <http://www.institutomarconi.com.br/pcc.htm>. [Accessed 21 February 2014].
- [7] G1 - Rio de Janeiro, "Petrobras afirma que informações sigilosas foram furtadas," Globo.com, 14 February 2008. [Online]. Available: http://g1.globo.com/Noticias/Economia_Negocios/0,,MUL298824-9356,00-INFORMAC OES+SIGILOSAS+SAO+FURTADAS+DA+PETROBRAS.html. [Accessed 21 February 2014].

- [8] Ponemon Institute. "The Cost of a Lost Laptop" INFO Online, 09 February 2009. [Online]. Available: <http://www.intel.com.au/content/dam/doc/whitepaper/enterprise-security-the-cost-of-a-lost-laptoppaper.pdf>. [Accessed 21 February 2014].
- [9] COMPUTERWORLD, "Pesquisa: Gestores de TI admitem vasculhar e-mails privados de funcionários," 26 May 2007. [Online]. Available: <http://computerworld.com.br/seguranca/2007/05/29/idgnoticia.2007-05-29.8374230723/>. [Accessed 21 February 2014].
- [10] P. Q. d. Almeida, "Códigos e Criptografia," 10 September 2010. [Online]. Available: <http://www.mat.uc.pt/~pedro/lectivos/CodigosCriptografia1011/>. [Accessed 20 December 2014].
- [11] L. R. KNUDSEN, "Block Ciphers — A Survey," in *State of the Art in Applied Cryptography*, Belgium, Springer Berlin Heidelberg, 1999, pp. 18 - 48.
- [12] R. Thomas, "Attacks on PGP: A User's Perspective," 2003. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/vpns/attacks-pgp-users-perspective-1092>. [Accessed 2014].
- [13] OPSWAT, "OPSWAT," [Online]. Available: <https://www.opswat.com>. [Accessed 01 March 2015].
- [14] A. G. GALLIANO, "O método científico: teoria e prática," São Paulo, Editora Mosaico, 1979, p. 6.
- [15] D. E. DENNING, "An Intrusion-Detection Model," IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, pp. 222 - 232, FEBRUARY 1987.
- [16] M. E. Delamaro, J. C. Maldonado and M. Jino, *Introdução ao Teste de Software*, 1 ed., vol. 1, Rio de Janeiro: Elsevier, 2007.
- [17] G. Aggarwal, E. Bursztein, C. Jackson and D. Boneh, "An Analysis of Private Browsing Modes in Modern Browsers," USENIX, 11 - 13 August 2010. [Online]. Available: <http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf>. [Accessed 30 June 2012].
- [18] Microsoft Corp., "Ten Immutable Laws Of Security," [Online]. Available: <https://technet.microsoft.com/en-us/library/hh278941.aspx>. [Accessed 22 February 2014].
- [19] C. Sanders, "How I Cracked your Windows Password (Part 1)," 20 January 2010. [Online]. Available: http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/How-Cracked-Windows-Password-Part1.html. [Accessed 20 February 2014].
- [20] Bloomberg Business, "The Problem with Password," 27 January 2011. [Online]. Available: http://www.bloomberg.com/bw/magazine/content/11_06/b4214036460585.htm. [Accessed 25 March 2013].
- [21] R. de S. Ruiz, F. P. Amatte and K. J. B. Park, "Security Issue on Cloned TrueCrypt Containers and Backup Headers," in *Proceedings of the International on Cyber-Crime Investigation and Cyber Security*, Kuala Lumpur, Malaysia, 2014.

ABOUT THE AUTHORS



Rogério Winter is a Colonel in the Brazilian army with more than 25 years experience in military operations and information security. He received a Master's degree in Electronic Engineering and Computation Aeronautics Institute Technological-ITA and is a member of the SDIWC (The Society of Digital Information and Wireless Communications). Today, he is dedicated to cyber warfare, command and control, and decision-making process and coauthor of the book "*Apoc@lypse: The End of Antivirus*". Email: rogwinter@gmail.com



Rodrigo Ruiz is a researcher at CTI – Information Technology Center - Renato Archer, Campinas, Brazil. He is also a member of the SDIWC (The Society of Digital Information and Wireless Communications) and co-author of the book "*Apoc@lypse: The End of Antivirus*" and many papers about privacy and security (https://www.researchgate.net/profile/Rodrigo_Ruiz3). Email: rodrigoruiz@outlook.com

Lazarus: Data Leakage with PGP and Resurrection of the Revoked User

Rodrigo Ruiz¹ and Rogério Winter²

¹*CTI Renato Archer, Campinas, Brazil*

²*Brazilian Army, Campinas, Brazil*

E-mail: rodrigoruiz@outlook.com; rogwinter@gmail.com

Received 8 September 2016; Accepted 10 November 2016;
Publication 19 November 2016

Abstract

The cybersecurity is the issue on the international agenda. The abuse of communication and faulty software is a common practice that brings the decade of 70. Invariably technology is the great protagonist of data leakage and loss of privacy. However, issues related to cybersecurity are founded on sociotechnical approach: technology, people, processes and environment, which interact indistinctly in a sensitive relationship. In this intricate sociotechnical environment of cybersecurity, this paper discloses a flaw in Symantec Encryption Desktop (SED), which can allow the leakage of sensitive information from governments, military and research centers around the world. In this context, as an example, the National Aeronautics and Space Administration (NASA) uses the Symantec Pretty Good Privacy (PGP) Encryption Desktop (SED). The Technology is not the main culprit for data leakage. Sometimes, the users are influenced by sophisticated marketing campaigns, which reaffirms the quality of products and services. In practice, this work is focused in the design errors and past vulnerabilities which are still present in recent technological solutions and allow data leakage and loss of privacy in a general way.

Keywords: Data Leakage, Privacy, Data Loss, Drive Encryption, Encryption, PGP, Symantec, NASA.

Journal of Cyber Security, Vol. 5.2, 1–14.

doi: 10.13052/jcsm2245-1439.521

© 2016 River Publishers. All rights reserved.

1 Introduction

First of all, we would like to explain the name of our article “Lazarus: Data Leakage with PGP and Resurrection of the Revoked User”. We used the biblical metaphor Lazarus history, regarding his return from death after a miracle. By the same token, we can resurrect a user revoked by the system administrator – as a miracle. However, user revoking resurrection have not the same consequence joy, as Lazarus resurrection.

Data leakage and Loss of Privacy are often used interchangeably to refer to a type of security breach that traditionally causes great financial losses and moral damages. The privacy issue and data loss in the digital world are sometimes controversial and difficult to solve because the cause is not so easy to detect. The intricate environment of cyber security is contaminated by issues that go beyond technology, gathering a quaternary structure composed by processes, people, environment, and technology. The reliability of a security system is based on temporally human knowledge concepts which are renewed, ratified or rectified day to day. In this paper, we test Symantec Pretty Good Privacy (PGP) Symantec Encryption Desktop (SED) and identified a vulnerability which permit information leakage. In this way, it is possible to show that the SED does not protect as it should, research laboratories, governments, agency, industry, armed forces etc. The cybersecurity is a complex problem and technology is not always accountable. The guiding principles behind information security are summed up in the acronym CIA, standing for Confidentiality, Integrity and Availability. We want our information to be read by only the right people (confidentiality), only be changed by authorised people or processes (integrity) and, be available to read and use whenever we want (availability).

Everybody needs to keep safety secrets, such as account password, state secrets, trade secrets, weapons project, aerospace projects, and new technologies. As a solution aiming keeping secrets – protection against cybercriminals, the user acquires cybersecurity solutions software & hardware, since any loss or leakage of information may cause serious damages such as reputation, financial losses etc.

Cybercriminals have stolen passwords from internet users...A survey conducted by InsightExpress and Cisco (CISCO, 2008), pointed out what IT professionals perceive about companies’ data loss incidents and answer why we need to protect our secrets:

70% of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies’ data loss incidents.

44% of employees share work devices with others without supervision.

39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

46% of employees admitted to transferring files between work and personal computers when working from home.

18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy.

Surveys such as conducted by the DSS Company (Filatovs, 2014) are very common and normally highlight special product features. A Symantec report presents that 10% of employees lost company devices such as computers and flash drives, however, 32% did not report these losses.

The above researches show the existence of an environment which is dark and uncertain. Moreover, manufacturers often exaggerate with promises ensuring highly efficient protection, perhaps beyond real security. Under certain circumstances, this assurance can hide threats. Some faults are difficult to detect, such as enabling revoked users in cryptosystems. In this case, attackers can enable revoked users allowing them to have access to cryptosystem again. Research Institute are attacked by hackers due to the nature of his activity.

"Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA and research laboratories." (The New York Times, 2005).

Recent publications on failures in many cryptographic applications systems allow access to private data. According to Security Issue on Cloned TrueCrypt Containers and Backup Headers (Ruiz, Amatte, & Park, 2014) and (Winter & Ruiz, Corrosive Secrecy and Confidence: the Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security, 2016) it is noteworthy how failures can compromise information security and privacy of people.

This paper is organized into the following sections: Introduction, Method, Attack Scenario, Results, and Discussion. In the introduction we contextualize the subject within the cybersecurity. In the Method section is shown in a didactic way the techniques used to explore the SED failure. In the Attack Scenario, we propose a plausible attack scenario due to the form of use indicated by Symantec. In the Results section, we present the results of operations of the SED and in the Discussion section we address some possibilities to fix the problem.

2 Method

Basically, we need three things to guarantee a privacy and protect the secrets from people or organizations: cryptography algorithms, application software, and people attitude.

- a. Cryptographic algorithms – This is the strongest resource. The algorithms are based on mathematical proofs which guarantee the maturity and system consistency. We may consider an attacker aiming to break an algorithm, he must expend much effort. The PGP and the Advanced Encryption Standard (AES) are good examples of cryptographic algorithms.
- b. Application Software – Cryptographic algorithms are used in conjunction with software application. Software application facilitates the usability, and allows deploy various algorithms. Examples of software application: Symantec Encryption Desktop (SED), Truecrypt, Veracrypt, Cipher-shed, Microsoft Bitlocker, and Bitdefender Total Security 2015 File Encryption.
- c. People attitude – People need to guarantee principles behind information security, such as: confidentiality, integrity and availability. On the other hand, they must use secure methods to store the information and to reduce the number of people that know a particular information. Moreover, a security policy will determine the rules for people and which features allowed.

An analysis of the items above – a, b, c – we consider that the major weaknesses may be found in application software and people attitude. A sociotechnical approach to cybersecurity seems more appropriate. Thus, the SED (Symantec Corporation, 2015) was chosen in this research the following reasons:

- The SED is based on PGP which is well-known algorithm and it has a high reliability and security.
- The Symantec developed SED as a user-friendly interface to a collaborative multi-user work. According to (CISCO, 2008), the humans are also responsible by exploration of software vulnerabilities. The SED facilitates collaborative work with security, but users need to follow a few security rules;
- The SED creates a protected virtual encrypted drive as a simple logical drive f:\. However, the access control of this PGP drive is assured by means of the management of cryptographic keys.

We highlight in this paper some software application and it is possible to note that all software share the same characteristic as SED. All tested application software use the same principle that is, the header section where it is stored user information and cryptographic keys. In this case, the software application allows the header to be manipulated to insert and revoke users. However, the vulnerability discovered on SED multi-user (Figure 1) permits full access in files even after PGP key was revoked by administrator user.

The method used in this article was the manipulation of the virtual encrypted drive header. The same method was applied to the software applications, such as: TrueCrypt (Ruiz, Amatte, & Park, 2014) and Bitdefender Total

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
50	47	50	64	55	53	45	52	74	01	00	00	6B	45	C9	2C	PGPdUSERt keE,
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	3C	00	00	00	38	01	00	00	00	00	00	00	< 8
00	00	00	00	00	00	00	00	00	00	00	00	55	53	45	52	USER
53	59	4D	4D	38	01	00	00	00	00	00	00	00	00	00	00	SYMM8
00	00	00	00	00	00	00	00	00	00	00	00	75	73	65	72	user
32	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	90	A9	DD	E3	0Y&
70	B2	71	4A	B5	D7	45	EB	5F	92	05	54	D9	54	CD	2B	p²qJp×Ee_ T0Tf+
D5	CF	31	76	37	8C	9B	C7	3B	EF	EC	68	00	00	00	00	0I1v7 Ç;iih
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	EA	F7	E6	70	é+ap
21	91	DE	7B	CB	FD	13	44	C9	CA	5E	AA	80	3E	00	00	l'p{Eý DÉÊ^> >
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 1 SED file with user segment permit the replacement. It is possible to make the revoked user returns.

Encryption 2015 (Winter & Ruiz, Luke 8:17 – Errors that Compromise the Privacy and Information Security, 2015).

In the mentioned article, all cryptographic system use a header to open the encrypted data. Basically, the SED file has two sections: header section and a data section. The header section has serious problems because this enables mixing of different file versions and permit to gain access to new file version. As SED is a multi-user system it needs to save in the same file all users' keys and encrypted data.

In this point, we show how to replace of headers of different versions of SED file. The method used to exploit the vulnerability exists in SED follows operation sequence below. Schematically the method follows as Figure 2 and Table 1:

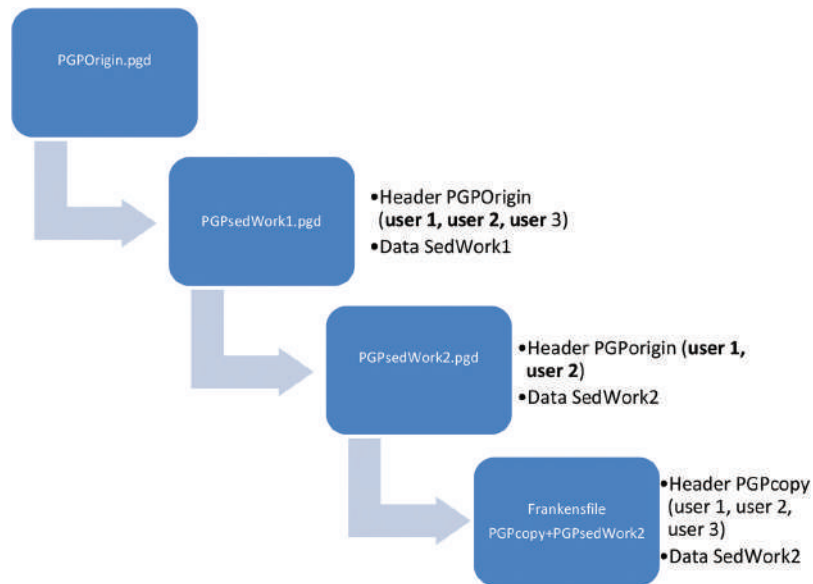
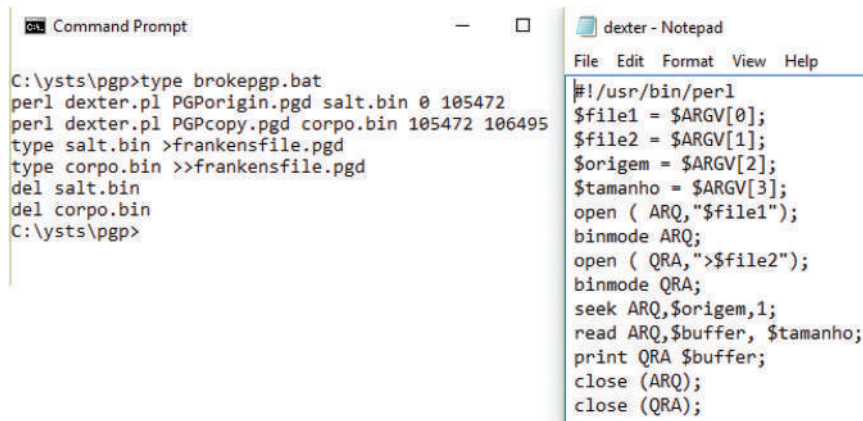


Figure 2 Process of file handling to create Frankensfile.pgd and information disclosure.

Table 1 Files, users and data type

File	Users	Data
PGPOrigin.pgd	user1, user2, user3	none
PGPcopy.pgd	user1, user2, user3	none
PGPsedWork1.pgd	user1, user2, user3	Secret text
PGPsedWork2.pgd	user1, user2	Secret text
Frankensfile.pgd	user1, user2, user3	Secret text

- Generate **PGPOrigin.pgd** file and create users (user1, user2 and user3);
- Make a copy of **PGPOrigin.pgd** into **PGPcopy.pgd**.
- Save the information inside the **PGPsedWork1.pgd** file. User1, user2 and user3 have access;
- Delete the user3 according SED user manual (Symantec, s.d.) from **PGPsedWork1.pgd** file. In theory, only user1 and user2 will have access to encrypted data.
- Make the **Frankensfile.pgd** file, which has the header section of **PGPcopy.pgd** and data section from **PGPOrigin.pgd** (Figure 2). Based on Figure 3, it is possible to reproduce the experiment using following file: Perl script dexter.pl and bat script brokepgp.bat.



The screenshot shows two windows. On the left is a Command Prompt window titled 'Command Prompt' with the following commands:

```
C:\ysts\pgp>type brokepgp.bat
perl dexter.pl PGPorigin.pgd salt.bin 0 105472
perl dexter.pl PGPcopy.pgd corpo.bin 105472 106495
type salt.bin >frankensfile.pgd
type corpo.bin >>frankensfile.pgd
del salt.bin
del corpo.bin
C:\ysts\pgp>
```

On the right is a Notepad window titled 'dexter - Notepad' showing the contents of the dexter.pl script:

```
#!/usr/bin/perl
$file1 = $ARGV[0];
$file2 = $ARGV[1];
$origem = $ARGV[2];
$tamanho = $ARGV[3];
open ( ARQ,"$file1");
binmode ARQ;
open ( QRA,">$file2");
binmode QRA;
seek ARQ,$origem,1;
read ARQ,$buffer, $tamanho;
print QRA $buffer;
close (ARQ);
close (QRA);
```

Figure 3 Perl script dexter.pl and bat script brokepgp.bat description.



The screenshot shows a Command Prompt window with the following output:

```
C:\ysts\pgp>md5sums *.pgd

MD5sums 1.2 freeware for win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                                MD5 sum
-----
[C:\ysts\pgp\]
frankensfile.pgd                                1327c98bb22cb38a8ad097dd3d54a7bf
PGPcopy.pgd                                     9531060b86ef7a925726bca4ac4954a9
PGPorigin.pgd                                  735806aa9de281d48746bd01ed4227b4
C:\ysts\pgp>
```

Figure 4 MD5 hash PGPOrigin.pgd, PGPcopy.pgd and Frankensfile.pgd.

- (f) The script Perl dexter.pl is responsible for divide files in two equal parts: header and data. On the other hand, the bat script **brokepgp.bat** is responsible for making the junction of header **PGPcopy.pgd** with data **PGPorigin.pgd** file. This scripts works in specific SED file conditions of size, file system and Encryption algorithm, but the principle is the same for all file configuration.

3 Attack Scenario

When starting an important project security administrators of the fictitious ACME Company configured a SED (**PGPorigin.pgd**) for the following users involved with the project: Peter, Tom and Sarah. From then on, they can save on the security of important project information within the SED file.

On the first day of the project, Sarah back up the SED file (PGPcopy.pgd) in a flash memory.

The three users (Peter, Tom and Sarah) working for months on the important ACME project saving the files within the SED (**PGPsedWork1.pgd**).

After six months, the user Sarah is fired from ACME Company and your login is deleted from the SED file (PGPsedWork2). However, it should be emphasized that Sarah still has the SED file (**PGPcopy.pgd**) which it was back up on the first day of the project and she can access the information. The logins of other users (Tom and Peter) are changed. In this case, the security issues are in compliance with the guidelines of the manufacturer, because the Saha user credentials do not allow access to the SED file (**PGPsedWork2**).

After his resignation, Sara is hired by a competing company ACME which it has interests in the same area of ACME project. As mentioned above, the cybersecurity has an engagement areas that extend beyond technological issues of software solution. In the Cisco Report (CISCO, 2008), 39% of companies surveyed had problems with employees who had access to unauthorized parties network or other service company. In addition, the same survey showed that 44% of employees share work devices with others without supervision.

In this way, it is reasonable to imagine that the file from ACME Company can be obtained by an unauthorized person. In this case, the SED file (**PGPsedWork2**), in which Sarah user does not have access credentials, but based on the information in the section Method, Sarah again get access to SED file.

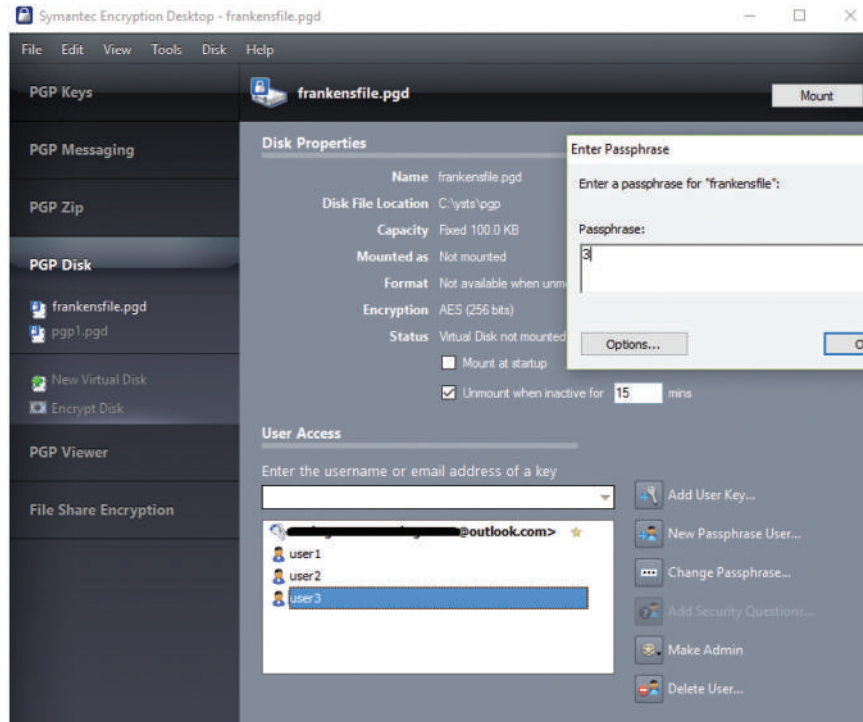


Figure 5 Frankensfile can open PGP1 file secrets with user3 revoked in pgp1.pgd.

4 Results

After of the steps method (Figure 2), user3 gained to the encrypted file **Frankensfile.pgd** Remembering that the user3 had their rights revoked earlier. The delete operation represented the resignation or termination of an employee from a project. In this case, a former employee (user3) who not had access to **PGPsdWork2.pgd** file now can read the encrypted information (**Frankenstyle.pgd**) with a simple file operation mixing.

5 Discussion

The cybersecurity is often weakened by beliefs, marketing advertisements or human behavior.

According to the article published in the CIO Magazine (Corbin, 2016), mentions that compliance is not the only way to ensure the security of

systems. Today's attacks are extremely sophisticated and exploit the weak protection systems, which was designed for more than a decade. The goal of software testing is highlighted defects if they exist. However, the results can be subject to modification, which depends on the method and the way that tests are performed. According to Forbes (Greenberg, 2010), Symantec paid \$300Million for PGP technology. Since then, Symantec has been using the algorithm in their security products. The fame of PGP has been used to give a reliability of cryptographic systems. However, as described above it is possible to access the contents of the files encrypted with PGP, regardless of the date of creation. We discovered the flaw in the SED, it is a flaw in the application software that uses PGP to encrypt the files. Probably the failure reported in this article is related a bug SED project, in the same way as in other systems mentioned above.

As a proposal to resolve this failure would be an encryption operation of the SED data file, when the user is deleted. In this way, it is possible to prevent the Header manipulation, as shown in the section Method.

The cybersecurity is based on people, technology, process and environment and the SED is basically a system that is subject to interference from 4 dimensions. Denning (E. Denning, 1987) observes that the major part of existing systems have vulnerabilities which make them susceptible to attacks, invasions and other kinds of abuse; moreover, the maintenance to avoid all such deficiencies is not viable technically nor economically.

After we discover this vulnerability, the Symantec Company was notified by protocol SSG15-044. In addition, we have identified that the National Aeronautics and Space Administration (NASA, 2012) uses the encryption system of Symantec PGP (Figure 6). Immediately, the NASA was informed by email about this vulnerability.

6 Conclusion

In this article our main goal is to alert scientists, governments and businesses around the world, just as we have done for Symantec and NASA on the risks of this type of security breach. According to TechNavio (Ellacott, 2014), the Symantec Company appears as a world leader in cybersecurity market and certainly the systems are used in thousands of government agencies, businesses and military.

Although Symantec video (Symantec Corporation, 2014) share the SED security premises, unfortunately we need to review the practice of information security. People, Companies and Research Labs around the world are feeling

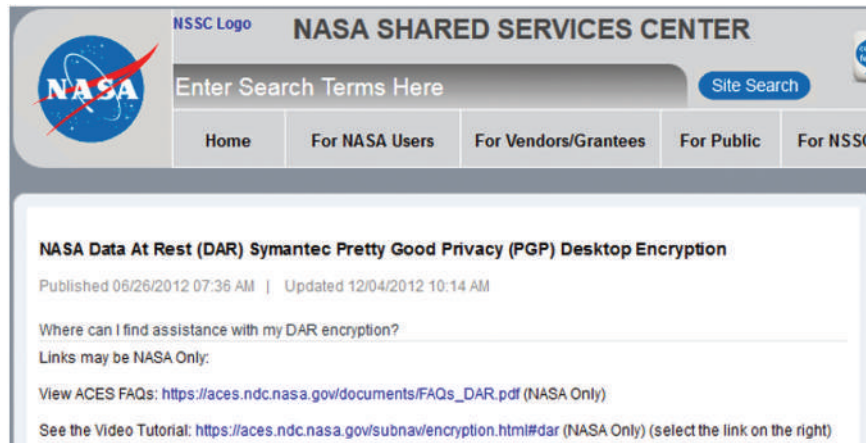


Figure 6 NASA screenshot with instructions about use PGP file encryption.

more secure when deploy cryptographic software to protect their information. The cybersecurity is more complex than the simple use of a cryptographic software. Scientists, governments and public institutions are living with a false sense of security using a vulnerable systems.

It is recommended that vendor require the SED to redo encryption whenever a user is deleted. This simple measure would prevent parts of an old file was used as a key to opening new files.

References

- [1] CISCO. (2008). *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. Available at: Data Loss Prevention: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html (Retrieved: February 24, 2014).
- [2] Corbin, K. (2016). *Cybersecurity much more than a compliance exercise*. Available at CIO: <http://www.cio.com/article/3025452/cyber-attacks-espionage/cybersecurity-much-more-than-a-compliance-exercise.html> (Retrieved February 24).
- [3] Denning, D. E. (1987). "An Intrusion-Detection Model," in IEEE (Ed.) *IEEE Transactions on Software Engineering – Special Issue on Computer*, Vol. 13, (Piscataway, NJ, USA: IEEE Press), 222–232. doi:10.1109/TSE.1987.232894

- [4] Ellacott, J. (2014). *Leading Email Encryption Vendors Respond to Heartbleed Bug Threat*. (Infiniti Research Limited). Available at: TechNavio: <http://www.technavio.com/report/global-email-encryption-market-2014-2018> (Retrieved February 22, 2015).
- [5] Filatovs, A. (2014). *Data Security Solutions*. Available at: Slide Share: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress-2014-arrowecs-roadshow-baltics> (Retrieved February 25, 2015).
- [6] Greenberg, A. (2010). *Symantec Acquires Encryption Provider PGP For \$300 Million*. (Forbes) Retrieved February 24, 2015, from Forbes Magazine: <http://www.forbes.com/sites/firewall/2010/04/29/symantec-acquires-encryption-provider-pgp-for-300-million/>
- [7] NASA. (2012). *NASA Data At Rest (DAR) Symantec Pretty Good Privacy (PGP) Desktop Encryption*. (NASA). Available at: NASA SHARED SERVICES CENTER: https://answers.nssc.nasa.gov/app/answers/detail/a_id/6235/~/%28nasa-data-at-rest-%28dar%29-symantec-pretty-good-privacy-%28pgp%29-desktop-encryption (Retrieved April 24, 2015).
- [8] Ruiz, R., Amatte, F. P., and Park, K. J. (2014). *Security Issue on Cloned TrueCrypt Containers and Backup Headers*. Kuala Lumpur, Malaysia: SDIWC. Available at: <https://www.researchgate.net/publication/271498536>
- [9] Symantec Corporation. (2014). *Symantec Endpoint Encryption – Protect Your Data*. (Google Inc.) Available at: You Tube: <https://www.youtube.com/watch?v=NtGSX3pYkLQ> (Retrieved February 24, 2015).
- [10] Symantec Corporation. (2015). *How Endpoint Encryption Works*. Available at: from Symantec Enterprise: http://www.symantec.com/content/en/us/enterprise/white_papers/how-endpoint-encryption-works_WP_21275920.pdf (Retrieved February 24, 2015).
- [11] The New York Times. (2005). *Nytimes*. Available at: http://www.nytimes.com/2005/05/10/technology/internet-attack-called-broad-and-long-lasting-by-investigators.html?_r=0 (Retrieved 01 05, 2016).
- [12] Winter, R., and Ruiz, R. (2015). Luke 8:17 – Errors that Compromise the Privacy and Information Security. *Def.camp*. Bucharest.
- [13] Winter, R., and Ruiz, R. (2016). Corrosive secrecy and confidence: the paradox among bypassing cryptographic software, loss of privacy and information security. *Cyber Secur. Rev.* 66–74.

Biographies



R. Ruiz is researcher of CTI – Information Technology Center – Renato Archer, Campinas, Brazil, also he is a member of the SDIWC (The Society of Digital Information and Wireless Communications) have some papers about privacy and he is co-author of *Apoc@lypse: The End of Antivirus* and he is author of papers about privacy and security.

https://www.researchgate.net/profile/Rodrigo_Ruiz3



R. Winter is colonel at the Brazilian Army with more than 25 years of experience in military operations and cybersecurity. He is master degree in Electronic Engineering and Computation by Aeronautics Technological Institute-ITA, also he is a member of the SDIWC (The Society of Digital Information and Wireless Communications) and at present, one dedicates to the warfare issues, cybernetics, command and control, and decision-making process and he is co-author of *Apoc@lypse: The End of Antivirus*.

CYBERSECURITY, CYBER WEAPONS AND CYBER-ATTACKS: RESPONSIBILITY AND DIFFERENT REFLECTIONS ON THE SUBJECT

By Rogério Winter, Colonel, Brazilian Army
and Rodrigo Ruiz, researcher, CTI - Information Technology Center Renato Archer

INTRODUCTION

Cybersecurity has been worrying governments, armed forces and society in general but this is not a recent issue. In October of 1971, Ron Rosenbaum published in the “Esquire” magazine a history so incredible that left the companies of telephony sad. In the article entitled “Secrets of the Little Blue Box,” Rosenbaum taught how it was possible to explore the various “hidden codes” of telephone exchanges using only a regular telephone. Perhaps this is the first account of a malicious way to exploit critical infrastructure, telephony. Since then, thousands of other events related to cybersecurity have succeeded to the present day.

WHAT IS THE CYBERSPACE?

The cyberspace is an environment with a high level of abstraction and the immediate consequence is the difficulty in identifying events and establishing their meanings in the kinetic (physical) domain. The cyberspace has the asymmetric characteristic that allows a balance of forces among countries with different military power. Likewise, the asymmetry of cyberspace modifies the social and human relations of citizens. Because anyone with programming knowledge can cause some kind of harm in civilian and military infrastructures.

In general, users of information technology have many questions about how to avoid data loss. There is no perfect solution for maintaining information security thus several rules or paradigms were created to mitigate data loss. A questionable paradigm, it is just install an anti-malware solution, preferably its inscribed on a comparative test list, and the protection is almost perfect.

It is a fact that issues about cyber-security should have a holistic look that integrates technology, processes, people and the environment. In the cyber environment, the attacker has tactical advantages, such as surprise, initiative and knowledge of a point of failure. Thus, during an attack, the observations of the facts can be ambiguous and this ambiguity will allow that counterattacks can be directed to structures of communications with cybernetic weapons as against physical structures with the use of kinetic weapons. Allied to this ambiguity of the environment between defence and attack cybernetic weapons have the great advantage of reuse of the weapon. On the other hand, even if you cannot reuse a cyber weapon to its fullest, using reverse techniques, you can identify which vulnerabilities the weapon tries to exploit. The Stuxnet used multiple zero-days, which allowed other attacks around after the attack on Natanz.

An attack that endangers critical infrastructure, both military and civil, will require retaliation or a pre-emptive strike against the risk of imminent attack, in a discriminatory and proportional manner.

“Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology – including the Internet – networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats.”^[1]

a. No constraints of physical space

The lack of perception of physical boundaries in the digital world hampers actions to combat cyber-terrorism and cybercrime as communication networks interconnect globally with a flow of information with little control. The nature of the internet makes it difficult to control where information travels.

b. Authorship assignment

After a cyber-attack, the identification of the aggressor is determinant so that an effective response can be imposed. However, in cyberspace the attribution of an attack is difficult, if not impossible, due to the various routes between communication networks.

c. Power asymmetries

One of the most interesting features in cyberspace is the power asymmetries. Where cleverness, subtlety, and cunning are as important as the economic and military power to carry out a cyber-attack.

d. Transversality of influence

In the military field, cyberspace is considered a domain that transcends all existing domains: earth, sea, air and space. In July 2016, during the Warsaw Summit^[2], NATO officially recognised cyberspace as an operational military domain. This means that the NATO alliance will respond with conventional weapons during the event of a cyber-attack. In this way, NATO is confirming that the Internet is a new battlefield.

e. Volatility

The volatility where the nature, speed, and dynamics of change are persistent.

f. Uncertainty

The uncertainty that leads to the lack of predictability, surprise and a sense of awareness and understanding of issues and events.

g. Complexity

The complexity is the difficulty of determining the chain of cause and effect and the confusion that surrounds the organisation. Cyberspace is an environment with a high level of abstraction and an immediate consequence is the difficulty of identifying events and establishing their meanings in the kinetic (physical) space.

h. Ambiguity

Ambiguity influences a misunderstanding of the meanings and leads to the confusion of cause and effect.

WHAT IS A CYBER WEAPON?

This paper accepts the definition proposed by Thomas Rid and Peter McBurney^[3]: “cyber weapon is a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings. The use of a cyber weapon is one way to conduct a cyber-attack. Clay Wilson^[4] in his article mentions the recent studies regarding cyber-attacks, which revealed common features that describe a cyber weapon:

- a. A malware attack campaign can combine multiple malicious programs for espionage, data theft or sabotage;
- b. The stealth capability allows you to maintain the secrecy of the operation for a long period;
- c. The attacker has detailed knowledge about the operation of the target system;
- d. There is a special kind of computer code to bypass cybersecurity protection technologies.

By the way, the cyber weapon has some advantages over kinetic weapons, such as:

- a. A cyber weapon needs less financial resources to be produced.
- b. It is possible use the same cyber weapon to attack different countries, organisations and governments.
- c. There is the difficulty of assigning the attacker.
- d. It is reasonable to reuse a cyber weapon against the attacker.
- e. The effects of a cyber weapon can transcend cyber space and cause kinetic effects.

CYBER STRATEGIES

Currently, we can observe that cybersecurity actions are fundamentally based on the versatility and dynamism to solve these problems, thus, the multidisciplinary teams involved is a preponderant factor of success. In this aspect, the ability to attribute and assign the authorship of a cyber-attack has intrigued police authorities, governments and security companies. The assignment is not always readily available, but eventually defenders can obtain enough information to take action.

Recently, there is evidence that minor attacks were performed as part of a main attack. This type of action is part of military strategies. For instance, Russia's operational military doctrine is based on the principle of "combined weapons", whereby each weapon of military service is used in a complementary relationship, so that weapons can be brought to victory. Successive military leaders throughout history used the principles of war. The best known of the early strategists was the legendary Chinese general and military theorist, Sun Tzu, who lived around 500-400 B.C. In this sense, the same tactics of conventional warfare can be adapted for cyberspace. The FM 100-5 Operations^[5] is an important reference in terms of military manoeuvre. Distracting and confusing the enemy is a very old and effective operation to reduce the defences of the main target. The digital world tends to imitate the real world; for instance, Apoc@lypse, the end of antivirus^[6] is the book where a bioinspired technique can be used as a cyber weapon.

GOVERNMENT RESPONSIBILITIES

To defend against cyber threats, countries around the world are building the most varied types of partnerships, such as training, legal agreements, technological development in cyber capabilities. These partnerships are constructing a new concept with goals to prepare and conduct combined cyber operations, i.e. to respond effectively against cyber threats and to detain and to defeat aggression in cyberspace.

The governments of the different countries have most recently been demanding cyber solutions, whether for monitoring terrorists, combating cybercrime or espionage. Some companies like Hacking Team, FinFisher GmbH, Elbit Systems and Vupen Security have developed solutions of attack and surveillance for governments and armed forces. However, buying cyber solutions from companies may not be the safest strategy because companies can have their systems hacked and attackers can expose buyers' information. This happened with Hacking Team, FinFisher GmbH, Elbit Systems and Vupen Security.

Intelligence agencies are apparently developing their own cyber weapons arsenal in order to take advantage in the various operations. Since 2013, Edward Snowden has disclosed details about NSA cyber operations against its enemies and NSA are using experts to identify failures in software and hardware. This is demonstrated in the reports released by Wikileaks and DoD's own reports.

In 2016, NASA was informed that its encryption system was vulnerable^[7], and it is believed the vulnerability persists. The subject is reported in the article "Lazarus: Data Leakage with Pretty Good Privacy and Resurrection of the Revoked User".

On May 2017, the world witnessed a cyber-attack that affected more than 200,000 computers in 150 countries^[8]. The attackers, an anonymous group called Shadow Brokers, based cyber weapon, Wannacry, on National Security Agency (NSA) leaked vulnerabilities in April.

In March 2017, WikiLeaks released information leaked from U.S. Central Intelligence Agency (CIA), code-named "Vault 7". It was the largest ever publication of confidential documents on the agency^[9].

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
05911928752	54	5A	3D	2D	32	26	65	66	64	43	53	52	3D	38	30	30
05911928768	78	36	30	30	26	75	73	65	72	6E	61	6D	65	3D	75	73
05911928784	72	63	69	74	69	26	75	73	65	72	6E	61	6D	65	4D	61
05911928800	73	6B	65	64	3D	75	73	2A	2A	2A	74	69	26	70	61	73
05911928816	73	77	6F	72	64	3D	63	69	74	69	70	61	73	77	74	2E
05911928832	BA	D5	D6	56	A9	96	14	00	78	3A	58	06	D0	0F	53	00
05911928848	70	6F	73	69	74	6F	72	79	30	0D	06	09	2A	86	48	86
05911928864	F7	0D	01	01	05	05	00	03	81	81	00	76	E1	12	6E	4E
05911928880	4B	16	12	86	30	06	B2	81	08	CF	F0	08	C7	C7	71	7E
05911928896	66	EE	C2	ED	D4	3B	1F	FF	F0	F0	C8	4E	D6	43	38	B0
05911928912	B9	30	7D	18	D0	55	83	A2	6A	CB	36	11	9C	E8	48	66
05911928928	A3	6D	7F	B8	13	D4	47	FE	8B	5A	5C	73	FC	AE	D9	1B
05911928944	32	19	38	AB	97	34	14	AA	96	D2	EB	A3	1C	14	08	49
05911928960	B6	BB	E5	91	EF	83	36	EB	1D	56	6F	CA	DA	BC	73	63
05911928976	90	E4	7F	7B	3E	22	CB	3D	07	ED	5F	38	74	9C	E3	03
05911928992	50	4E	A1	AF	98	EE	61	F2	84	3F	12	00	EC	16	39	CF
05911929008	12	B1	77	DB	EF	45	D5	21	B1	D4	D7	5D	73	97	14	0E
05911929024	68	00	74	00	74	00	70	00	73	00	3A	00	2F	00	2F	00
05911929040	6D	00	65	00	74	00	72	00	69	00	63	00	73	00	31	00
05911929056	2E	00	63	00	69	00	74	00	69	00	62	00	61	00	6E	00
05911929072	6B	00	2E	00	63	00	6F	00	6D	00	2F	00	62	00	2F	00

Figure 1: User credentials recovered from Citi.com in clear text.

In September 2017 the article “The leakage of passwords from home banking sites: A threat to global cyber security?”^[10] described the vulnerability in the credential control system of several banks around the world. This failure allows the home banking user information to be stored on the computer in clear text so that an attacker can retrieve them and perform bank transactions. Figure 1 clarifies how Citi’s home banking credentials are retrieved in clear text. This vulnerability can also be found on several e-commerce sites, e-mail, intranet systems, government services and the military.

Cyber threats threaten not only public institution but also society, business, government, and the military. This becomes more critical when we realise that governments have not yet taken a concrete step towards improving cybersecurity of society. Is cybersecurity a matter to be evaluated and discussed from the point of view of state? Or society or maybe both?

From the examples cited above, there is a marked need for governments to participate in guiding the various protective actions of society. In this context, the United Nations Security Council is the body of the United Nations whose mandate is to ensure the

maintenance of international peace and security. The United Security Council consists of 15 members, with five permanent members with veto power: the United States, France, the United Kingdom, and the People’s Republic of China. We emphasise in this regard that Article 27 of the Charter of the United Nations allows permanent members to use their right of veto to block decisions of the Security Council. However, war is a lucrative business. According

to Stockholm International Peace Research¹, world military expenditure was estimated at \$1686 billion in 2016, equivalent to 2.2 per cent of global gross domestic product or \$227 per person. The same report presents the ten countries that most exported weapons: USA, Russia, China, France, Germany, UK, Spain, Italy, Ukraine, and Israel. Here a paradox is established, since the countries that have the responsibility to maintain world peace are those that export most arms.

When a war artifact is launched and fails to reach a target, the military protocol establishes the destruction of artifact. In the military unit, there is a professional EOD team² responsible for assessing the situation and destroying the device that failed. In a recent example in Germany³, thousands of residents were forced to evacuate a Frankfurt district on Sunday (September 03, 2017) before experts began the operation at a construction site where the device was found earlier in the week. However, in the cyber environment the situation is somewhat different. To conduct a disruptive or destructive cyber operation against a military system or industrial control system requires only expertise and a potential adversary

1 <https://sipri.org/sites/default/files/2017-09/yb17-summary-eng.pdf>

2 Explosive Ordnance Disposal (EOD Team) EOD team have expert knowledge, skills and equipment.

3 <http://www.dw.com/en/frankfurt-evacuates-thousands-to-defuse-world-war-ii-bomb/a-40343581>

rather than spending 10 billion dollars to develop an offensive capability. To build a cyber weapon needs more of people's intelligence and less investment than a kinetic weapon. This can equilibrate the world war game. In addition, a cyber weapon can be reused against an attacker with some improvements. Acting shrewdly is as important as economic and military power to carry out a cyber-attack. Anyone can learn how to create effective cyber weapons. For this, all that is necessary is a computer, Internet connection, time to learn about software, hardware network vulnerabilities, and finally patience. In the examples mentioned above it is possible to identify the contribution of governments to producing an insecure cyber environment. How are governments dealing with this?

CONCLUSION

Nowadays, our society depends on efficient and security computer systems. However, we realise that governments have not yet taken a concrete step toward coordinating the cybersecurity in our society. In addition to the aspects mentioned in this article, there are issues that are difficult to solve internationally: internet censorship, anonymity on the internet and attribution of attacks; applicability of existing laws of war to cyberspace; overflow effect of cyber attacks and protection of intellectual property.

Between the 1970s and 1990s, the world had a geopolitical polarisation, and armed conflicts were geographically delimited – only nations was engaged in warfare. Critical infrastructure control systems were not reliant on technology, and cybercrime and cyber espionage were not so obvious.

Since the 1990s, new paradigms have emerged. Geographical barriers no longer exist for political militancy, social media and electronic media democratised the information. Vital systems are increasingly complex and dependent on information technology. Nations, corporations and organised groups began to use cyber space to carry out war activities

and claim rights. The various information technologies became cheap and easily accessible to all.

Cybersecurity is the issue on the international agenda. The abuse of communication and faulty software is a common practice that brings the decade of 70. Invariably, technology is the great protagonist of data leakage and loss of privacy. However, issues related to cybersecurity are founded on social, anthropological and technical approach: technology, people, processes and environment, which interact indistinctly in a sensitive relationship. Insiders contribute to the dissemination of information and there are flaws in information security processes. Denning^[11] mentioned in her article that developing systems that are absolutely secure is extremely difficult, if not generally impossible. Because the concepts used today to developing system may in the future be outdated. There are many flaws hidden in the systems. For instance, Microsoft patches critical bug that affects every Windows version since 95⁴ and this flaw existed for almost 19 years. Are concepts in computer science consolidated or are they eventually reviewed and questioned?

Again, Denning^[11] emphasised that existing systems with known flaws are not easily replaced by systems that are more secure – mainly because the systems have attractive features that are missing in the more-secure systems, or cannot be replaced for economic reasons. In November 2015, the Paris Orly Airport⁵ had to close temporarily after the failure of a system running Windows 3.1. In addition, UK's Nuclear Submarines⁶ used windows XP in 2016. Unquestionably, both cases justify our premise.

Unlike conventional weapons, cyber weapons do not require much in the way of financial resources and on many occasions governments are contributing to the development and spread of cyber weapons. Saved to the right proportions, in cyber war countries are using their economic power to buy, discover and store zero-day vulnerabilities of software and hardware

4 <https://www.theverge.com/2014/11/12/7202801/microsoft-patches-critical-19-year-old-windows-bug>

5 <https://arstechnica.com/information-technology/2015/11/failed-windows-3-1-system-blamed-for-taking-out-paris-airport/>

6 <https://mspoweruser.com/uks-nuclear-submarines-runs-windows-xp-submarines/>

systems. We define zero-days as the raw material of cyber weapons. Another interesting characteristic of the cyber weapon is re-use of the weapon against its own attacker. After a cyber-attack, specialists can capture the cyber artefact and with some changes or improvements, it is possible to fight back. In this case, act shrewdly and precisely is as important as the economic and military power to carry out a cyber-attack.

War is a profitable business and the environment of insecurity helps to maintain a business model of fear^[11]. We may conclude that all governments are contributing to an insecure cyber world. We have no victims in this game. All of our countries are responsible for global cyber-attacks. All countries will continue to improve their cyber weapons. The DOD should continue to prioritise its cyber investments and develop the capabilities required to defend U.S. interests at home and overseas^[12]. What can we expect of cybersecurity? ■

REFERENCES

- [1] NATO, "Cyber Definitions," NATO, 2007. [Online]. Available: <https://ccdcoc.org/cyber-definitions.html>. [Accessed 26 09 2017].
- [2] North Atlantic Treaty Organisation (NATO), "Warsaw Summit Communiqué," NATO, 09 July 2016. [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber. [Accessed 01 september 2017].
- [3] T. Rid and P. McBurney, "Cyber-Weapons," RUSI Journal, vol. 157, pp. 6-13, 29 February 2012.
- [4] C. Wilson, "Cyber weapons: 4 defining characteristics," 04 June 2015. [Online]. Available: <https://gcn.com/articles/2015/06/04/cyber-weapon.aspx>. [Accessed 06 December 2015].
- [5] ARMY WAR COLL CARLISLE BARRACKS PA, "Defense Technical Information Center," 31 march 1986. [Online]. Available: <http://www.dtic.mil/docs/citations/ADA170781>. [Accessed 29 september 2017].
- [6] R. Ruiz, R. Winter, K. Park and F. Amatte, *Apoc@lypse: The End of Antivirus*, Charleston – US: Amazon, 2015.
- [7] R. Ruiz e R. Winter, "Lazarus: Data Leakage with PGP and Resurrection of the Revoked User," *Journal of Cyber Security and Mobility*, pp. 1-14, 04 2016.
- [8] D. Burg and S. Joyce, "Cybersecurity after WannaCry: How to Resist Future Attacks," PWC, 16 May 2017. [Online]. Available: <https://www.strategy-business.com/blog/Cybersecurity-After-WannaCry-How-to-Resist-Future-Attacks?gko=22163>. [Accessed 17 May 2017].
- [9] WikiLeaks, "Vault 7: CIA Hacking Tools Revealed," Wikileaks, 07 March 2017. [Online]. Available: <https://wikileaks.org/ciav7p1/>. [Accessed 22 May 2017].
- [10] R. W. K. P. F. A. Rodrigo Ruiz, "The leakage of passwords from home banking sites: A threat to global cyber security?," *Journal of Payments Strategy & Systems*, Volume 11 / Number 2 / Summer 2017, pp. 174-183, 09 2017.
- [11] R. Ruiz, "Symbiosis and fear: Evolutionary Benefits of Cybersecurity," *United States Cyber Security Magazine*, vol. 6, n° 1, pp. 109-111, 6 2017.
- [12] DoD, "The DoD Cyber Strategy," 2015.

ABOUT THE AUTHORS



Rogério Winter is a Colonel in the Brazilian Army with more than 25 years of experience in military operations and information security. He holds a Master's degree in Electronic Engineering and Computer Science at the Instituto Tecnológico de Aeronáutica (ITA) - Brazil and is a member of the Society of Digital Information and Wireless Communications. His current interests are warfare issues, cybernetics, command and control, and decision-making processes. He is also the co-author of 'Apoc@lypse: The End of Antivirus'.



Rodrigo Ruiz is a researcher at CTI - Information Technology Center Renato Archer, Campinas, Brazil. In addition, he is the IEEE member, member of SDIWC, as well as the co-author of *Apoc@lypse: The End of Antivirus*. He has also authored papers about privacy and

security for *Cyber Defense Magazine*, *Cyber Security Review*, *US Cyber Security Magazine*, *JPSS*, *IJOFCs*, *JCSM* and international conferences and Journals.
Contact: rodrigoruiz@outlook.com
https://www.researchgate.net/profile/Rodrigo_Ruiz3

CALL FOR PAPERS

Critical Infrastructure Protection Review editorial team would like to invite government departments, intergovernmental organisations, researchers, academics and industry experts to contribute their articles, case studies, research papers and opinion pieces.

We are looking for both theoretical and practice based non-promotional editorial contributions. Only original, so far not published articles are accepted.

All enquiries and articles should be submitted by email to: editorial@deltabusinessmedia.com

For more information please visit: <http://www.criticalinfrastructureprotectionreview.com/editorial/>

CRITICAL INFRASTRUCTURE PROTECTION REVIEW

Unique content | Global reach | In print and online

PRINT EDITION



WEBSITE



NEWSLETTER



eBOOK AND PDF



DISTRIBUTION AT THE EVENTS



Keep up-to-date with the latest news and developments,
subscribe at <http://www.criticalinfrastructureprotectionreview.com/subscribe/>



Rodrigo Ruiz



Rogério Winter



Kil Jin Brandini Park



Fernando Amatte

The leakage of passwords from home banking sites: A threat to global cyber security?

Rodrigo Ruiz*, Rogério Winter,** Kil Jin Brandini Park[†] and Fernando Amatte^{††}

Received (in revised form): 14th April, 2017

*CTI Renato Archer, Rodovia Dom Pedro I (SP-65), Km 143,6, Amarais, Campinas SP, 13069-901, Brazil
E-mail: rodrigoruiz@outlook.com

**Brazilian Cyber Defense, Brazilian Army/CTI Renato Archer, Rodovia Dom Pedro I (SP-65), Km 143,6, Amarais, Campinas SP, 13069-901, Brazil
E-mail: rogwinter@gmail.com

[†]Computer Faculty, UFU, Federal University of Uberlândia, Campus Santa Mônica, Bloco 1^a, Sala 1A236 Av. João Naves de Ávila, 2.121, Bairro Santa Mônica, Uberlândia MG, 38400-902, Brazil
E-mail: kil.pos.seg@gmail.com

^{††}E-mail: famatte@gmail.com

Rodrigo Ruiz is researcher at Renato Archer Center for Information Technology and a member of the Society of Digital Information and Wireless Communications. He has presented at a number of conferences, and his work on privacy and security has been published in such journals as *Cyber Security Review Magazine*, *Cyber Defense Magazine*, *Journal of Cyber Security and Mobility*, *2600 Magazine*, *United States Cyber Security Magazine* and *International Journal of Cyber Security and Digital Forensics*. He is also a co-author of the book 'Apoc@lypse: The End of Antivirus'.

Rogério Winter is a colonel in the Brazilian army with more than 30 years' experience in military operations and information security. He is a member of the Society of Digital Information and Wireless Communications and has a master's degree in electronic engineering and computation from the Aeronautics Technological Institute. His work focuses on cyber warfare, decision-making processes and command and control. He is also a co-author of the book 'Apoc@lypse: The End of Antivirus'.

Kil Jin Brandini Park is a professor at the Federal University of Uberlândia, specialising in computer engineering and information security. He has a PhD in engineering and conducts

postdoctoral work in malware analysis. He is also a co-author of the book 'Apoc@lypse: The End of Antivirus'.

Fernando Amatte has more than 20 years of experience in security IT. He has a postgraduate qualification in information security and is a Certified Information Systems Security Professional, GIAC Certified Incident Handler and Módulo Certified Security Officer. His experience includes coordinating a security team for a large multinational bank, and coordinating automated malware analysis for the Pandora Project. He is also a co-author of the book 'Apoc@lypse: The End of Antivirus'.

ABSTRACT

E-banking systems rely on browsers and other financial applications to provide a secure service. As this paper shows, however, many e-banking systems fail to provide the requisite level of confidentiality. This paper focuses on vulnerabilities related to the leakage of login information from the client side. It demonstrates that by using forensic techniques and tools, it was possible to acquire login-related data from a number of websites. This proves that important authentication data used in navigation activities remain on disk, posing a clear threat to confidentiality.

Keywords: *privacy, credentials bank, browser forensic analysis, password management, bank account leakage data, credentials management*

INTRODUCTION

The ongoing assessment of operating systems, browsers and cryptographic programs has already generated many disclosures about security breaches and failures.^{1,2}

The present research focuses on the treatment of user login information (usernames and passwords) by major websites that provide services such as search, home banking, e-mail and e-commerce. Table 1 provides a list of the sites tested, with their economic activity classified according to UK Standard Industrial Classification (UK SIC) Codes.³

The data gathered for the present research provide important details about how these sites manage their users' passwords on the client side. Many different bank and retail websites have been tested and found to be vulnerable to password leakage. For ethical reasons, however, discussion of these vulnerabilities is outside the scope of the present paper.

This paper starts with a discussion on threats and vulnerabilities, and discusses other

research and methodological treatments in the context of this topic. The paper then describes the methods and tests used in this study. The results obtained by the tests are then presented and discussed. Finally, conclusions are drawn and recommendations for further studies are proposed.

THREATS AND VULNERABILITIES

First and foremost, it is important to understand the different kinds of security threat and threat sources as well as types of attack. In this respect, it is of paramount importance to define a set of characteristics that allow the classification of these attacks, threats and sources — ie an attack taxonomy. 'A taxonomy also allows for previous knowledge to be applied to new attacks as well as providing a structured way to view such attacks'.⁴ To accomplish this goal, Lough presents a taxonomy of computer attacks named VERDICT.⁵ The first four letters of the name stand for verification, exposure, randomness and deallocation, the four main characteristics used to classify such attacks:

- *verification*: attacks perpetrated when the proper data verification was not conducted;
- *exposure*: attacks perpetrated when data are unduly exposed;

Table 1: Sites tested

<i>Domain</i>	<i>Economic activity</i>
gmail.com	Information and communication
hotmail.com	Information and communication
yahoo.com	Information and communication
amazon.com	Retail trade
paypal.com	Financial and insurance activities
ebay.com	Retail trade
santander.com.br	Financial and insurance activities
walmart.com.br	Retail trade
bradesco.com.br	Financial and insurance activities
citibank.com.br	Financial and insurance activities
citibank.com	Financial and insurance activities
jpmorgan.chase.com	Financial and insurance activities
particulares.gruposantander.es	Financial and insurance activities

- *randomness*: attacks perpetrated when functionality that requires randomness displays a predictable pattern; and
- *deallocation*: attacks perpetrated when data are not deallocated correctly after usage, resulting in residuals.

In respect to this classification, Lough notes two main problems: generality and lack of classification in applying modern nomenclatures such as ‘virus’, ‘worm’ and ‘trojan’.⁶ Lough therefore proposes a new taxonomy based on the following dimensions:

- *base dimension*: applied to categorise the attack based on its vector or closest class in case there is no specific vector;
- *second dimension*: applied to categorise the attack based on its target;
- *third dimension*: applied to categorise the attack based on the vulnerabilities and exploits; and
- *fourth dimension*: applied to categorise the attack based on payloads and secondary effects.

Lough presents a list of definitions to help the classification of attacks with no obvious vector inside the base dimension. Of these, two are noteworthy: password attacks and information-gathering attacks. Attacks that fit these two definitions do not necessarily cause damage to data, but focus on information acquisition for further attacks.

Furthermore, inside the third dimension, Howard presents some categories of vulnerabilities, among them password vulnerabilities,⁷ while a technical report from the Carnegie Mellon Software Engineering Institute presents the CERT vulnerability taxonomy, which consists of design errors, implementation errors, user interface and other problems.⁸

On the same topic,⁹ Howard *et al.* propose the vulnerability called ‘failure to protect stored data’ and suggest that software developers tend to care more for data in traffic than for stored data, despite the fact

that data spend more time in storage than being transferred.

In discussing a taxonomy for malware that targets browsers, Sood and Enbody propose that targeting vulnerabilities in the privacy model is a distinct class of exploitation, in which one can find issues related to browser storage.¹⁰

In studies of browsers, one line of forensic tests methodology lies in the analysis of structures used by these applications. The alternative to the previous methodology is to search for forensic content on storage devices through the analysis of data format (eg signatures).

In a study about the private browsing feature, Ruiz *et al.* adopted the second line of methodology.¹¹ Applying signatures and string matching, the authors were able to extract data related to visited websites in various browsers even though the private browsing functionality was in use.

Given that HTTP protocol was designed to be stateless, there is a clear need for some way to correlate requests originating from the same user. HTTP cookies are one such mechanism to resolve this requirement. A vast amount of information can be stored on such structures, including site credentials (username and passwords), configuration preferences, session and cache data, and tracking information.¹²

Considering the importance of information stored inside cookies, Khu-Smith and Mitchell describe three classes of threat related to this structure:¹³

- the confidentiality of data stored inside cookies;
- the monitoring of users’ browsing habits through cookies; and
- the deployment of malicious applications through cookies.

In the first class, it is clear that unless some degree of protection is offered, credentials stored in cookies could become targets of information-gathering attacks.

In discussing authentication problems, Fu *et al.* present three categories of attack.¹⁴ In the first one, called existential forgery, an attacker can forge an authenticator for some unspecified user, which means that he cannot target one specific user. In the second class, called selective forgery, a specific user can be targeted. In the third and final class, called total break, an attacker is able to recover the user key and is therefore able to build valid authenticators at will.

The research discussed herein points to the existence and importance of attacks targeting authentication data. In addition, Oh *et al.* analyse a vast class of information about the navigation activities that browsers save to disk.¹⁵

Building on this, the present research will focus on vulnerabilities related to login information management relating to the usernames and passwords found on non-volatile memory.

METHODS AND TESTS

One major question permeates and guides the present research: what happens if a laptop or similar equipment with storage capability is stolen?

Furthermore, consider this basic html form:

HTML code

```
<form method='POST' action=''>
<br>User:<input type='text' name='user'
size='20'>
<br>Password: <input type='password'
name='password' size='20'>
<br><input type='submit'>
</form>
```

Where is the security behind it? How easy is it to access the usernames and passwords of bank, e-mail or e-commerce sites accessed?

Table 2 summarises the tests conducted as part of this research.

Table 2: Summary of the tests conducted as part of this research

Test name	Condition	Sites
A	Consists, on a virtual machine with Safari 5.1.7_1 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
F	Consists, on a virtual machine with Firefox 24.0_1 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
G	Consists, on a virtual machine with Google Chrome 30.0.159969M_1 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
M	Consists, on a real machine with Internet Explorer 10 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
AC	Consists, on a virtual machine with Android 4.0.3 and web browser Robot installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
O	Consists, on virtual machine with Opera 27.0.16.89.69 installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br
T	Consists, on virtual machine with Tor Browser installed, to access and sign in	gmail.com, hotmail.com, yahoo.com, amazon.com, paypal.com, ebay.com, santander.com.br, walmart.com.br and caixa.com.br

For tests A, F, G, O and T, a standard guest virtual machine (with the Windows 7 Pro operating system) in the host operating system (Windows 7 Pro) was created using Virtual Box.¹⁶ Windows was installed with the minimal resources, ie 25Gb of disk and 500Mb of main memory. In case any future work required comparison of the base guest machine with guest machines running the different browsers tested, an export (snapshot) of the newly installed Windows machine was created.

For test M, the Windows 7 Pro operating system was installed on bare metal.

Finally, for test AC, a guest virtual machine (with the operating system Android 4.0.3) was created in the host operating system (Windows 7 Pro) using Virtual Box.

The browsers tested were Internet Explorer 10, Firefox 24.0_1, Google Chrome 30.0.159969M_1, Safari 5.1.7_1, Opera 27.0.16.89.69, Robot 4.0.3 and Tor Browser 4.0.4.

For each test on the four setups, the private browsing function was turned on. Specifically, the following private browsing functions were activated: Internet Explorer's 'InPrivate', Firefox's 'Private Browsing', Chrome's 'Incognito', Safari's 'Private Browsing', Opera's 'Private Browsing' and Robot 'Incognito' functions. Tor Browser comes with default private browsing as the only possible configuration.

To proceed with data analysis, it is important to define the techniques available. In this respect, Carrier brings forth a series of considerations. If the analyst knows the address of the data, he will feed the analysis tool with the logical file system address and it will convert this information into the byte or sector address of the data unit. This technique is called 'by data unit viewing'.¹⁷

The other option is to know the general format of the data instead of the address or location of the data unit. In this case, one proceeds with logical file system level searching where the data units will be

searched for some particular information format or signature.

The present work adopts logical file system level searching. This being the case, the first step is to have or define a set of signatures.

As discussed previously, one class of vulnerability relates to information residuals — ie failure to maintain proper confidentiality safeguards with respect to stored data — whether said data be inside a specific browser structure or data file or simply inside transient files used by the application or operational system.

In the present case, the Foremost program,¹⁸ a renowned forensic tool for extracting ('data carving') files different of formats, is used to analyse the images of the virtual machines to search for information related to any usernames and passwords used on the listed websites.

The process of file carving one can be generalised as 'using a database of headers and footers (essentially, strings of bytes at predictable offsets) for specific file types [to] retrieve files from raw disk images, regardless of the type of filesystem on the disk image'.¹⁹ Furthermore, 'open source tools may more clearly and comprehensively meet the guideline requirements than would proprietary tools'.²⁰

Another search tool for specific keywords generated during the browsing activities, WinHex, 'is a universal hexadecimal editor tool, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security'.²¹

As these signatures had not been defined previously, the virtual machine's disk was opened with WinHex and a search for a singular password previously created for each site or service was conducted.

This technique made it possible to create a model (Figure 1) to configure the Foremost software and seek the header for all websites visited that contained the user's identification. Note that this study does not use any knowledge about structures used by browsers (eg cookies).

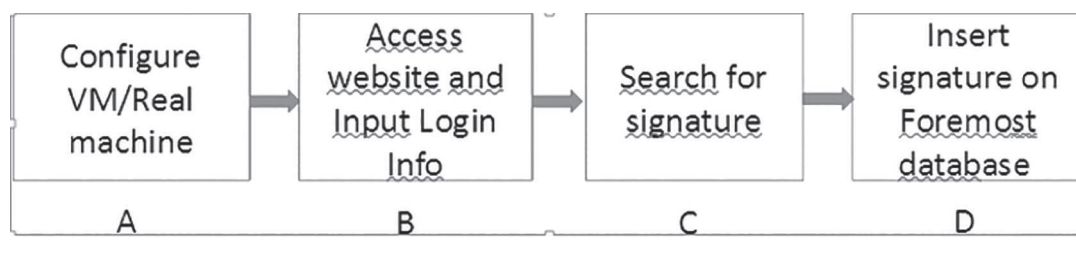


Figure 1 Signature extraction methodology

Table 3: Signature of the login information for some of the tested sites

Site	Signature
Hotmail	login=
Gmail	google.com/ServiceLoginAuth
eBay	kgct=&userid=
Santander	hdnPluginOK=&txtNome=
Amazon	&mail=

Table 3 presents some of those extracted signatures.

RESULTS AND DISCUSSION

The four selected browsers were used to log into the various sites listed. After completing the tests summarised in Table 3, Foremost was used to extract data samples from the virtual machine disk image and WinHex was used to identify the signatures.

Figures 2–9 show the recovered plain-text passwords from home banking, e-mail and e-commerce sites. The password is obliterated in Figures 4–6 and Figure 9 because the researcher used his real account and password.

When the site failed to hide its login data, it was possible to extract the password. This occurred with all browsers tested, which means that independent of the browser, Gmail, Amazon, eBay, Santander, Hotmail, Caixa and Citibank websites showed the same vulnerability.

As part of the study, many army and government sites were also tested; these also left the user's password as clear text.

After acquiring the forensic data, a deeper analysis was conducted on Windows OS to identify the files and directories that contained the recovered data.

In the case of Internet Explorer, the following directories and files contained the recovered information about authentication:

- \users\user\appdata\local\microsoft\Internet Explorer\recovery\last active\
- \users\usuário\appdata\local\microsoft\windows\temporary internet files\low\content.ie5\
- \Pagefile.sys

Aside from the operating system's paging process, Internet Explorer also leaks login information on structures used by the browser to store temporary files and information used to recover the last active browsing session.

In the case of Chrome, Firefox and Safari, the only file that contained the recovered information about authentication was Pagefile.sys. This proves that, in their case, the leakage of login information is caused by the operating system's paging process.

In the tests conducted with the site caixa.gov.br, the following files contained recovered information about authentication:

- \Program Data\gpplugin\cef\bank.gbl.??
- \users\usuário\appdata\local\microsoft\windows temporary\wk9???\adsadclient31.htm

The various site owners were contacted about these vulnerabilities. Caixa, in particular,

11875721168	50 E8 D8 32 00 00 83 C4 10 8D 44 24 18 50 8D 84	Pè02 Ä D\$ P
11875721184	24 6C 02 00 00 50 FF 15 58 10 00 10 8B 3D 5C 10	\$l Pÿ X =\
11875721200	00 10 6A 04 89 44 24 14 5B 83 F8 FF 0F 84 3A 01	j D\$ [øÿ :
11875721216	67 00 6F 00 6E 00 26 00 53 00 69 00 74 00 65 00	g o n & S i t e
11875721232	49 00 64 00 3D 00 43 00 50 00 42 00 4C 00 6F 00	I d = C P B L o
11875721248	67 00 6F 00 6E 00 00 00 00 00 02 00 00 80 04 00	g o n & S i t e
11875721264	3E 00 1E 00 00 00 00 00 00 00 00 00 00 00 AC AD	>
11875721280	AC AB 07 00 00 00 75 00 73 00 65 00 72 00 6A 00	~< user j
11875721296	70 00 6D 00 01 00 00 00 03 00 00 80 04 00 3E 00	p m >
11875721312	1E 00 00 00 00 00 00 00 00 00 00 00 AC AD 7C AB	~<~<
11875721328	07 00 00 00 70 00 61 00 73 00 73 00 6A 00 70 00	pass j p
11875721344	6D 00 01 00 00 00 04 00 00 80 04 00 3E 00 1E 00	m >
11875721360	00 00 00 00 00 00 00 00 00 00 AC AD AC AB 77 00	~<~<
11875721376	00 00 70 00 61 00 73 00 73 00 6A 00 70 00 6A 00	pass j p m
11875721392	01 00 00 00 05 00 00 80 04 00 3E 00 10 00 00 00	>
11875721408	00 00 00 00 00 00 00 00 54 52 53 54 FF FF FF FF	TRSTÿÿÿÿ
11875721424	01 00 00 00 06 00 00 80 04 00 3E 00 6A 07 00 00	> j
11875721440	00 00 00 00 00 00 00 00 06 AE AC AB AD 03 00 00	@~<~<
11875721456	7B 00 22 00 6E 00 61 00 76 00 69 00 67 00 61 00	{ " n a v i g a
11875721472	74 00 6F 00 72 00 22 00 3A 00 7B 00 22 00 61 00	t o r " : { " a
11875721488	70 00 70 00 43 00 6F 00 64 00 65 00 4E 00 61 00	p p C o d e N a
11875721504	6D 00 65 00 22 00 3A 00 22 00 4D 00 6F 00 7A 00	m e " : " M o z
11875721520	69 00 6C 00 6C 00 61 00 22 00 2C 00 22 00 61 00	i l l a " , " a
11875721536	70 00 70 00 4D 00 69 00 6E 00 6F 00 72 00 56 00	p p M i n o r V
11875721552	65 00 72 00 73 00 69 00 6F 00 6E 00 22 00 3A 00	e r s i o n " :
11875721568	22 00 30 00 22 00 2C 00 22 00 62 00 72 00 6F 00	" 0 " , " b r o
11875721584	77 00 73 00 65 00 72 00 4C 00 61 00 6E 00 67 00	w s e r L a n g
11875721600	75 00 61 00 67 00 65 00 22 00 3A 00 22 00 70 00	u a g e " : " p
11875721616	74 00 2D 00 62 00 72 00 22 00 2C 00 22 00 63 00	t - b r " , " c
11875721632	6F 00 6F 00 6B 00 69 00 65 00 45 00 6E 00 61 00	o o k i e E n a
11875721648	62 00 6C 00 65 00 64 00 22 00 3A 00 74 00 72 00	b l e d " : t r
11875721664	75 00 65 00 2C 00 22 00 63 00 70 00 75 00 43 00	u e , " c p u C

Figure 2: Recovered JP Morgan credentials 'userjpm' and 'passjpm'

responded promptly by modifying its login method. When the tests were applied for a second time, passwords could no longer be found on the hard disk in a clear text format. Indeed, it seems that it now applies some cryptographic function on the password before it is written to disk.

The results of this investigation suggest that attackers today do not need to install key-logger software and wait weeks for a possible result. Likewise, malware that

targets banks does not need to create a complex clone of bank websites. Using the method demonstrated by the present work, it is possible to obtain usable login data with a single click on a malicious link.

The problem is aggravated by the fact that if an attacker acquires an eBay or Amazon password, they can buy products using the 'one-click' purchase function, because the user's payment information is already bounded to their account.

w7-disk1.vmdk																	
[unregistered] w7-disk1.vmdk C:\Users\vsruiz\VirtualBox\		TZ=-2&efdCSR=800 x600&username=us rciti&usernameMa sked=us***ti&pas sword=citipaswt. 900v0 x:X B S pository0 *IH ÷ vá nN K 10 2 I3 ÇÇq~ fiAi0; ýäENÖC8+ 10} BU!ojE6 lèHf fm, ÖGpIZ\sü0 2 8<<14 3!Öëf I 1>ä'i16ë VoEÜksc ä {>"E= i_8t!ä PNI_!ia0! ? i 9I ±wüEÖ!±0x]s! h t t p s : / / m e t r i c s 1 . c i t i b a n k . c o m / b / s s / c i t i n a p r o d / 1 / H . 2 4 . 4 / s 3 3 2 6 8 6 6 8 5 5 7 7 4 5 ? A Q B = 1 & n d h = 1 & t = 6 % 2 F 1 1 % 2 F 2 0 1 3 % 2 0 8 % 3 A 2 2 % 3 A 3 0 % 2 0 5 % 2 0 1															
Offset		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
File size: 12.7 GB 13,611,499,520 bytes	05911928752	54	5A	3D	2D	32	26	65	66	64	43	53	52	3D	38	30	30
	05911928768	78	36	30	30	26	75	73	65	72	6E	61	6D	65	3D	75	73
DOS name\W7-DIS-1.VMD	05911928784	72	63	69	74	69	26	75	73	65	72	6E	61	6D	65	4D	61
	05911928800	73	6B	65	64	3D	75	73	2A	2A	2A	74	69	26	70	61	73
Default Edit Mode State: original	05911928816	73	77	6F	72	64	3D	63	69	74	69	70	61	73	77	74	2E
	05911928832	BA	D5	D6	56	A9	96	14	00	78	3A	58	06	D0	0F	53	00
Undo level: 0 Undo reverses: n/a	05911928848	70	6F	73	69	74	6F	72	79	30	0D	06	09	2A	86	48	86
	05911928864	F7	0D	01	01	05	05	00	03	81	81	00	76	E1	12	6E	4E
Creation time: 09/10/2013 12:44:04	05911928880	4B	16	12	86	30	06	B2	81	08	CF	F0	08	C7	C7	71	7E
	05911928896	66	EE	C2	ED	D4	3B	1F	FF	F0	F0	C8	4E	D6	43	38	B0
Last write time: 06/12/2013 08:35:00	05911928912	B9	30	7D	18	D0	55	83	A2	6A	CB	36	11	9C	E8	48	66
	05911928928	A3	6D	7F	B8	13	D4	47	FE	8B	5A	5C	73	FC	AE	D9	1B
Attributes: AX Icons: 0	05911928944	32	19	38	AB	97	34	14	AA	96	D2	EB	A3	1C	14	08	49
	05911928960	B6	BB	E5	91	EF	83	36	EB	1D	56	6F	CA	DA	BC	73	63
Mode: Text	05911928976	90	E4	7F	7B	3E	22	CB	3D	07	ED	5F	38	74	9C	E3	03
	05911928992	50	4E	A1	AF	98	EE	61	F2	84	3F	12	00	EC	16	39	CF
Character set: CP 1252 Offsets: decimal Bytes per page: 32x16=512	05911929008	12	B1	77	DB	EF	45	D5	21	B1	D4	D7	5D	73	97	14	0E
	05911929024	68	00	74	00	74	00	70	00	73	00	3A	00	2F	00	2F	00
Window #: 1 No. of windows: 1	05911929040	6D	00	65	00	74	00	72	00	69	00	63	00	73	00	31	00
	05911929056	2E	00	63	00	69	00	74	00	69	00	62	00	61	00	6E	00
Clipboard: available	05911929072	6B	00	2E	00	63	00	6F	00	6D	00	2F	00	62	00	2F	00
	05911929088	73	00	73	00	2F	00	63	00	69	00	74	00	69	00	6E	00
TEMP folder: 64.0 GB free C:\Users\vsruiz\Music	05911929104	61	00	70	00	72	00	6F	00	64	00	2F	00	31	00	2F	00
	05911929120	48	00	2E	00	32	00	34	00	2E	00	34	00	2F	00	73	00

Figure 3: Recovered Citibank US login 'usernameMasked=us***ti' and 'password=citipaswt'

Figure 4: Recovered Santander login located after marks 'txtNome=' and 'txtSenha='

67	69	6E	4F	4B	3D	26	74	hdnPluginOK=&txtNome=
61	3D	26	74	78	74	41	67	&txtSenha=&txtAg
31	39	26	74	78	74	43	6F	encia=&txtCo
--	--	--	--	--	--	--	--	nta=.

Figure 5: Recovered eBay login located after marks 'userid=' and 'pass='

72	66	78	3D	65	35	62	36	.0&bUrlPrfx=e5b6
37	69	6D	61	26	72	71	69	04141a3d7ima&rqi
30	34	31	34	31	30	61	35	d=a3e5b6041410a5
36	34	66	66	34	65	66	37	edcd94ca64ff4ef7
26	75	73	65	72	69	64	3D	62&kgct=&userid=
								&pass=
								&keepMeSi
6F	6E	3D	31	26	73	67	6E	gnInOption=1&sgn
69	6E	26	68	74	6D	69	64	Bt=Sign+in&htmid

Figure 6: Recovered Amazon login located after marks 'email=' and 'password='

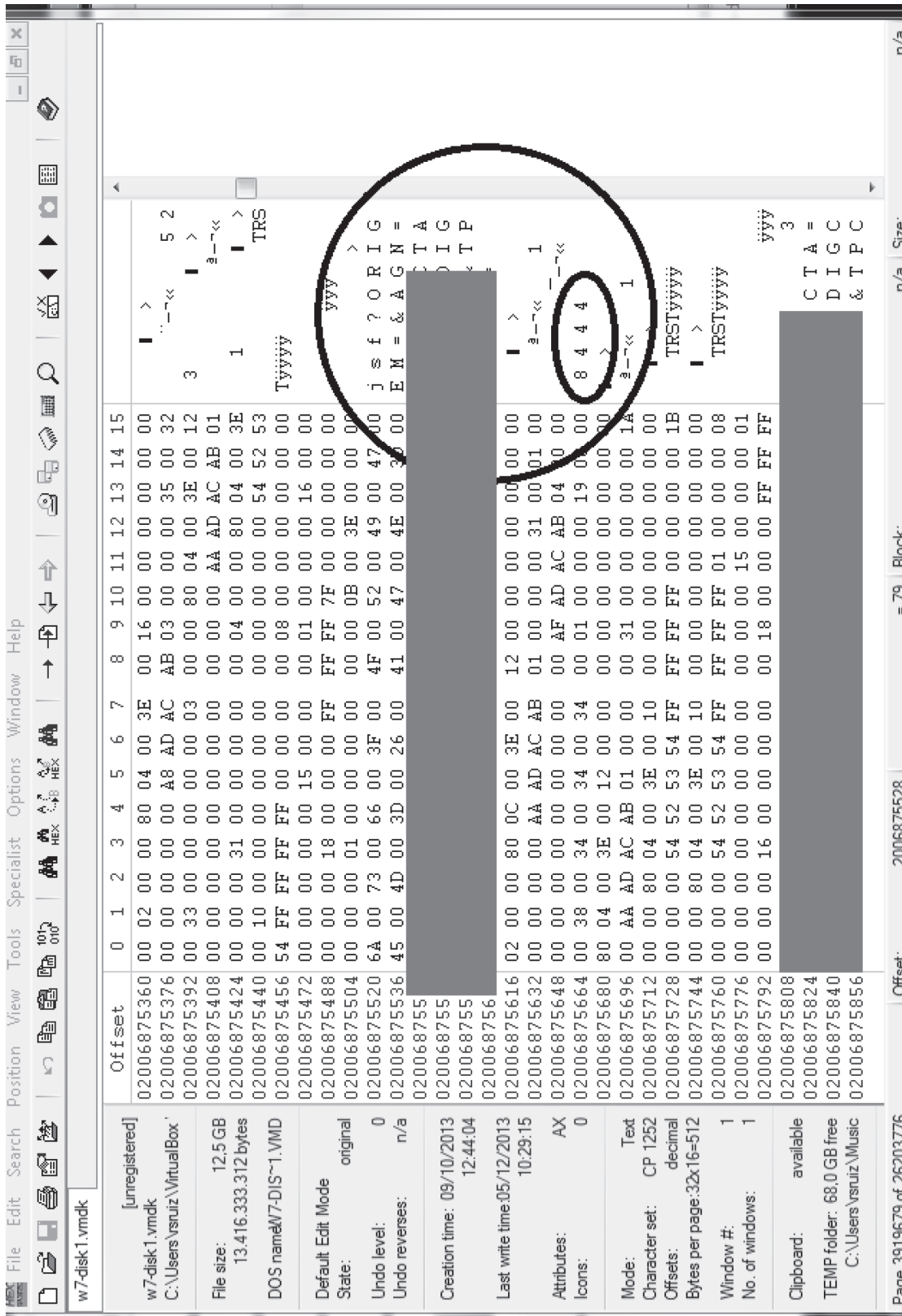
75	59	57	31	68	65	6D	39	6Ly93d3cuYW1hem9
6E	63	43	39	6A	63	33	4D	uLmNvbS9ncC9jc3M
68	5A	32	55	75	61	48	52	vaG9tZXBhZ2UuaHR
56	56	45	59	34	4A	6E	4A	tbD9pZT1VVEY4JnJ
76	58	33	6C	68	62	56	39	lZl89Z25vX3lhbV9
44	26	65	6D	61	69	6C	3D	5YQ%3D%3D&email=
								mail.com&create=
								0&password=
								metadata=1

77	00	45	00	4A	00	70	00	1	2	U	0	w	E	J	p
61	00	69	00	6C	00	3D	00	o	&	E	m	a	i	l	=
69	00	76	00	61	00	74	00	i	n	p	r	i	v	a	t
6B	00	40	00	67	00	6D	00	e	.	r	f	k	@	g	m
63	00	6F	00	6D	00	26	00	a	i	l	.	c	o	m	&
77	00	64	00	3D	00	71	00	P	a	s	s	w	d	=	
79	00	75	00	69	00	6F	00	w	e	r	t	y	u	i	o
26	00	73	00	69	00	67	00	p	#	9	9	&	s	i	g
4C	00	6F	00	67	00	69	00	n	I	n	=	L	o	g	i
72	00	73	00	69	00	73	00	n	&	P	e	r	s	i	s
43	00	6F	00	6F	00	6B	00	t	e	n	t	C	o	o	k
65	00	73	00	26	00	72	00	i	e	=	y	e	s	&	r
77	00	6E	00	3D	00	31	00								

Figure 7: Recovered Gmail login 'Email= inprivate.rfk@gmail.com' and 'Passwd = qwerty'

68	74	74	70	73	3A	2F	2F									https://
76	65	2E	63	6F	6D	2F	00									login.live.com/
73	3A	2F	2F	6C	6F	67	69									https://logi
6F	6D	2F	6C	6F	67	69	6E									n.live.com/login
68	74	74	70	73	3A	2F	2F									.srf(https://
76	65	2E	63	6F	6D	2F	70									login.live.com/p
70	6F	73	74	2E	73	72	66									secure/post.srf
6C	00	6F	00	67	00	69	00									l o g i
69	00	6E	00	70	00	72	00									n i n p r
65	00	5F	00	72	00	66	00									i v a t e _ r f
74	00	6C	00	6F	00	6F	00									k @ o u t l o o
6D	00	00	00	00	00	00	00									k . c o m
73	00	73	00	77	00	64	00									p a s s w d
32	00	33	00	34	00	35	00									@ 1 2 3 4 5
30	00	00	00	00	00	00	00									6 7 8 9 0

Figure 8: Recovered Hotmail login 'login inprivate_rf@outlook.com' and 'passwd @1234567890'



SOLUTION

Four levels of solution are proposed to address the vulnerability reported in this paper: operating system, web browser, frameworks and web developer.

The operating system must be changed to use cryptographic features to manage the swap memory. In this way, if a computer is inadvertently shut down, the user information will be saved and will not be recovered even with forensic operations.

Web browser operations need to be modified to protect the user because the operating system stores data on the hard drive without proper security handling. It is true that web browsers encourage users to enable private browsing functions. However, this option has already been explored elsewhere²² and can encourage a false sense of security as it is still possible to recover navigation data from the hard disk.

Framework vendors should update their frameworks so that login and password fields can be secured with encryption when saving user credentials.

Finally, web developers should consider security by design and review all site building codes and processes. All web system components must be tested to prevent failures and keep user data safe.

CONCLUSION

Online banking has become as commonplace as sending e-mails, as most banks now offer a variety of services, including transfers, bill payment, consultations, cards and loans, and so on. In addition to allowing the user to circumvent the long queues usually found in banking branches, internet banking is also a great way to avoid being affected by industrial action, which can leave thousands of clients without in-branch banking provision.

Clearly, banks too benefit from the provision of online banking. Automating routine bill payments, minimising the need to visit the bank in person and offering out-of-hours

banking services all reduce the time required for routine banking activities. It is therefore in the interest of banks to address the vulnerability discussed in this paper so that consumer confidence in their product is not adversely affected.

It bears repeating that most existing systems — whether financial applications or the web browsers used to support them — have security flaws that render them susceptible to intrusions, penetrations and other forms of abuse.²³ For technical and economic reasons, it is not feasible to find and fix all these deficiencies. This puts a greater onus of responsibility on users, as their security depends in no small part on their online behaviour. Indeed, regardless of where a failure is found in the operating system — in the https protocol, the web browser or application — the user must be cautious and must be aware that their credentials are at risk. They must also be aware of virtual scams such as phishing, and the like.

The vulnerability discussed in the present work and the process used to exploit it will work whether the disk space is a virtual or real disk. With this in mind, online banking users should be informed of the risks and should take precautions in order to better secure their access credentials themselves.

AUTHORS' NOTE

This research was performed in 2015. The results were delivered to the Brazilian Bank Federation FEBRABAN via private lecture at FEBRABAN headquarters. The report was also sent via e-mail to banks around the world, as well as to Microsoft, Google, Amazon and PayPal.

REFERENCES

- (1) Aggarwal, G., Bursztein E., Jackson C. and Boneh D., (2010) 'An analysis of private browsing modes in modern browsers', available at: <http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf> (accessed 30th June, 2012).

- (2) Carrier, B. (2005) 'File System Forensic Analysis', in 'File System Forensic Analysis', Pearson Education, Crawfordsville, IN, pp. 12–16.
- (3) Prosser, L. (ed.) (2009) 'UK Standard Industrial Classification of Economic Activities 2007 (SIC 2007)', published by Palgrave Macmillan for Office for National Statistics, Houndmills, Basingstoke.
- (4) Hansman, S. and Hunt, R. (2005) 'A taxonomy of network and computer attacks', *Computers & Security*, Vol. 24, No. 1, pp. 31–43.
- (5) Lough, D. (2001) 'A taxonomy of computer attacks with applications to wireless networks', unpublished PhD thesis, Virginia Polytechnic Institute.
- (6) *Ibid.*
- (7) Howard, J.D. (1997) 'An analysis of security incidents on the internet 1989–1995', unpublished PhD thesis, Carnegie Mellon University.
- (8) Seacord, R.C. and Householder, A.D. (2005) 'A Structured Approach to Classifying Security Vulnerabilities', Report No. CMU/SEI-2005-TN-003, Carnegie Mellon University, Pittsburgh, PA.
- (9) Howard, M., Leblanc, D. and Viega, J. (2009) '24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them', McGraw-Hill Education, Columbus, OH.
- (10) Sood, A. and Enbody, R. (2011) 'A browser malware taxonomy', *VirusBulletin*, available at: <https://www.virusbulletin.com/virusbulletin/2011/06/browser-malware-taxonomy/> (accessed 10th February, 2017).
- (11) Ruiz, R., Amatte, F. and Park, K.J.B. (2014) 'Opening the "private browsing" data — acquiring evidence of browsing', in 'Proceedings of the International Conference on Information Security and Cyber Forensics, Kuala Terengganu, 8th October', pp. 72–79.
- (12) *Ibid.*
- (13) Khu-Smith, V. and Mitchell, C. (2002) 'Enhancing the security of cookies', in Kim, K. (ed.) 'Proceedings of International Conference on Information Security and Cryptology (ICISC) 2001: Information Security and Cryptology, Seoul, 6th–7th December', Springer, Berlin and Heidelberg, pp. 132–145.
- (14) Fu, K., Sit, E., Smith, K. and Feamster, N. (2001) 'Dos and don'ts of client authentication on the web', in 'Proceedings of the 10th Conference on USENIX Security Symposium, 13th–17th August', USENIX Association, Washington, DC, p. 19.
- (15) Oh, J., Lee, S. and Lee, S. (2011) 'Advanced evidence collection and analysis of web browser activity', in 'Proceedings of the 8th Annual Digital Forensics Research Conference, New Orleans, LA, 1st–3rd August', pp. S62–S70.
- (16) Oracle (2014) 'Oracle Virtual Box', available at: <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html> (accessed 15th November, 2014).
- (17) Carrier, B. (2002) 'Packet Storm', available at: http://dl.packetstormsecurity.net/papers/IDS/atstake_opensource_forensics.pdf (accessed 25th November, 2014).
- (18) Kornblum, J., Kendall K. and Mikus N. (2002) 'Foremost', available at: <http://foremost.sourceforge.net/pkg/foremost-1.5.7.tar.gz> (accessed 12th October, 2012).
- (19) Richard III, G.G. and Roussev, V. (2005) 'Scalpel: a frugal, high performance file carver', in 'Proceedings of the 2005 Digital Forensic Research Workshop (DFRWS), New Orleans, LA, 17th–19th August', pp. 1–10.
- (20) Carrier, ref. 17 above.
- (21) X-Ways Software Technology AG (2014) 'WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor', available at: <http://www.x-ways.net/winhex/> (accessed 10th November, 2014).
- (22) Ruiz R, *et al.*, ref. 11 above.
- (23) Denning, D. E. (1987) 'An intrusion-detection model', *IEEE Transactions on Software Engineering*, Vol. 13, No. 2, pp. 222–232.

Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life

Rogério Winter¹, Rodrigo Ruiz²

¹ Brazilian Army / CTI Renato Archer

Campinas – Brazil

rogwinter@gmail.com

rogerio.winter@cti.gov.br

² CTI Renato Archer

Campinas – Brazil

ORCID 0000-0003-1644-3933

rodrigoruiz@outlook.com

rodrigo.ruiz@cti.gov.br

ABSTRACT

Viruses are a major threat to the health of people because can trigger diseases. With regard to cybersecurity, viruses that attack computers and they are difficult problems to solve. Computer viruses as well as human viruses have evolved over the years. Computer Viruses are human creations and they are product of their creativity and ingenuity. The current antivirus systems are protect software and use various techniques to combat cyber threats, however we have discovered a way to by-pass its protection. Inspired by the concepts of viral infection and prophage we can to start an autoimmune disease in an antivirus system. An autoimmune disease is a condition arising from an abnormal immune response to a normal body part. Thereby, we start the cyber autoimmune disease and the antivirus system is responsible for destroying the computer's operating system. The proof of concept was called Apoc@lypse Technique and it was tested successfully with 56 antivirus system brands.

KEYWORDS

Autoimmune; Antivirus; Trust; Cyber Terrorism; Cyber weapon; Project Fail

1 INTRODUCTION

"Viruses are the most abundant parasites on Earth" [1]. Well-known viruses, such as the flu

virus, attack human hosts, while viruses, such as Sasser, Conficker, and Stuxnet infect computer. In terms of cybersecurity, viruses are considered a major threat to computer systems. Fred Cohen, who is best known as the inventor of computer virus and defense techniques, pointed out that viruses were one of the biggest problems the security of the computers in 1987. Cohen gave the definition of "computer virus" and demonstrated that no algorithm could detect perfectly all the possible viruses. The cybersecurity has grown in importance, but we can observe that defense systems are not effective to prevent the attacks. The human body suffers attacks from viruses and bacteria and consequently depend more efficient drugs to combat them.

It is remarkable proximity between the virtual world and the real world, perhaps because the problems of computing solutions have been inspired by the observation of nature itself. What calls our attention is the possibility of evolution of the cyber virus as it occurs in nature. Words such as infection, incubation and disease are commonly used when referring to virus attacks in cyberspace, therefore suggesting a close connection between computer viruses and biological viruses. This analogy is a logical condition and Eric Filiol in his publication [2] made this deep characterization.

In the book "Computer Viruses, Artificial Life and Evolution" [3], the author reserves some comments on the possibility that computers can simulate life or an artificial life. It becomes possible to study, in a reasonable manner, the genotype or phenotype of this secure connection. Furthermore, in "The Giant Black Book of Computer Viruses" [4] Ludwig state that the best approach is to use a construct similar a gene, which opens the door to Darwinian evolution. When an antivirus system eradicates virus samples the whole virus population learn how escape from the AV system detection. This phenomenon can be called a simple Darwinian evolution. Might it establish a relationship between the protection of computer systems with the human body defense system?

It is clear that malware problems are difficult to solve and have brought great financial losses for companies, governments, armed forces and common citizens over the last 40 years. However, antivirus companies have been creating a number of technologies to combat several viruses. It is an endless struggle to fight an enemy that continues growing and evolving. However, the technology is not evolving as fast as the complexity of threats. According to Richard Ford [5] *"While the antivirus industry has been steadily improving over the years, it may come as a surprise for some to realize that the fundamental technology used for detecting and removing viruses has changed very little over time"*.

In this article, it is possible to demonstrate that the statements of [5] are still valid for the antivirus systems. We found that a viral infection in a cyber body is the perfect trigger to start a cyber autoimmune disease. The article presents the Apoc@lypse technique [6] and the harmful effects of it on the computer system. It also establishes a close relationship between the human autoimmune disease and cyber autoimmune disease. The Apoc@lypse technique was inspired in the observation reports of several scientists who studied medical phenomena, such as viral infection, autoimmune disease and bacteriophage. Apoc@lypse technique is equivalent to program bacteria using a technique inspired by the bacteriophage to carry a virus fragment until the

cells. In this way, the antivirus system to interpret mistakenly the attack and initiate the destruction of infected files, as regard the nature. Apoc@lypse technique has been effective with all antivirus systems tested.

2 APOC@LYPSE TECHNIQUE

Nowadays, virus are considered as a subclass of malwares. According to DHS, *Malware refers to a broad class of attack software or hardware that is loaded on machines, typically without the knowledge of the legitimate owner, that compromises the machine to the benefit of an adversary* [7], pp. 38. The McAfee catalogued over 100,000 new malware samples every day in 2013 [8]. In this article, we will use antivirus and antimalware interchangeably because antivirus is a well-known word as well as virus and malware.

Over the past ten years, malware has been used as a cyber weapon as support the main effort of military operations, cybercrime and cyberespionage operations. For instance, in 2010 the Stuxnet malware was used for the first large-scale attack on Supervisory Control and Data Acquisition (SCADA) in Natanz Nuclear Plant at Iran. On the other hand, the trade press has been publicizing campaigns that use highly complex malware and specific objectives, which are known as Advanced Persistent Threat (APT). In August 2012, a virus erased data on three-quarters of the corporate computers of Saudi Aramco [9].

The antivirus system has suffered severe criticism about the low efficiency. Some articles in the trade press have decreed the death of the same. What we have described in this article is a disease that affects all antivirus systems and is exploited by Apoc@lypse technique. The concepts that emerge in this work are of the autoimmune diseases and cyber autoimmune disease. *Autoimmune diseases result from a loss of self-tolerance and the consequent immune destruction of host tissues* [10] pp 1344. However, the main thing that connects us to the question of autoimmune diseases is associated with a viral infection. There are indications that

some viral infection can induce or exacerbate autoimmune diseases [10].

Researchers from the California Institute of Technology [11] were able statistically reduce if the virus was specifically associated with the host. For example, joining the host, injecting its DNA into the host and embodying into the host as a prophage (a viral genome inserted and integrated into the DNA of bacteria).

Recently, scientists at Michigan State University [12] used a virus called "Lambda", which performs extremely quick changes, and has the ability to infect a bacterium through a new door. Typically, the lambda virus is capable of infecting E. coli cells. Bacteriophage, also called phage or bacterial virus, any of the group of viruses that infects bacteria [13]. Phages replicate within the bacterium following the injection of their genome into its cytoplasm.

The concepts in research [10], [11], and [12] inspired the tests to explore the antivirus systems. Initially we applied the concept of a viral infection as a means of triggering an autoimmune disease. Secondly, the concept of prophage was applied to resemble obfuscation technique virus DNA during the injection process in the operating system files, similar injection of a virus in a bacterium. Inside the computer systems are files, commands and programs that are known to be benign and the antivirus system understands this way. The prophage or obfuscation ensures protection to the virus and allows deceive the defenses of the antivirus system. Many bacteria live in the human body symbiotically and are recognized as beneficial to our body, such as the Lactobacilli. Thus, the bacteria do not sensitize the human immune system.

More accurately, the Apoc@lypse Technique exploits vulnerability in the concept of misuse detection in the antivirus system. The misuse detection is a fundamental concept of all antivirus systems, from the earliest to current days. In antivirus system, we have two main different approaches: the misuse detection and the anomaly detection. Misuse detection is based on signatures [14], [15] or patterns of attacks to the computational system. Some actions directed to the objects of the

system are considered as threatening, such as file deletion, hard disk formatting or attempts to modify privileged access files. Well-defined and known actions to the weak points of a system form the signature of the attacks. The detection of attacks happens by observing such actions occurring with specific objects. Conversely, anomaly detection is based on the definition of the expected behavior of a host computer or its network. Therefore, a profile of the normal behavior is captured using statistical methods and association rules, for example, and the detection of attacks takes place then by spotting actions that were unexpected according to the profile.

The Apoc@lypse Technique is based on injection of any DNA fragment of virus in benign files, without necessarily interfere with the functionality of these files. Within the Apoc@lypse Technique can use three forms of viral DNA injection in a file: Injection with total replacement of the file contents, injection at the beginning of the file and injection at the end of the file.

Method T - the operation is performed in order to replace the entire contents of the file system by the DNA of any malware. Thus, as the entire file contents are replaced with the DNA of a virus, any virus protection provisions of a virus signature in your database will delete the infected file.

Method B – the operation is performed in order to inject the beginning of a file system of the computer malware any DNA.

Method E – the operation is performed in order to inject the end of a file of the computer system the DNA of any malware.

Figure 1 schematically represents the method of injection settings:

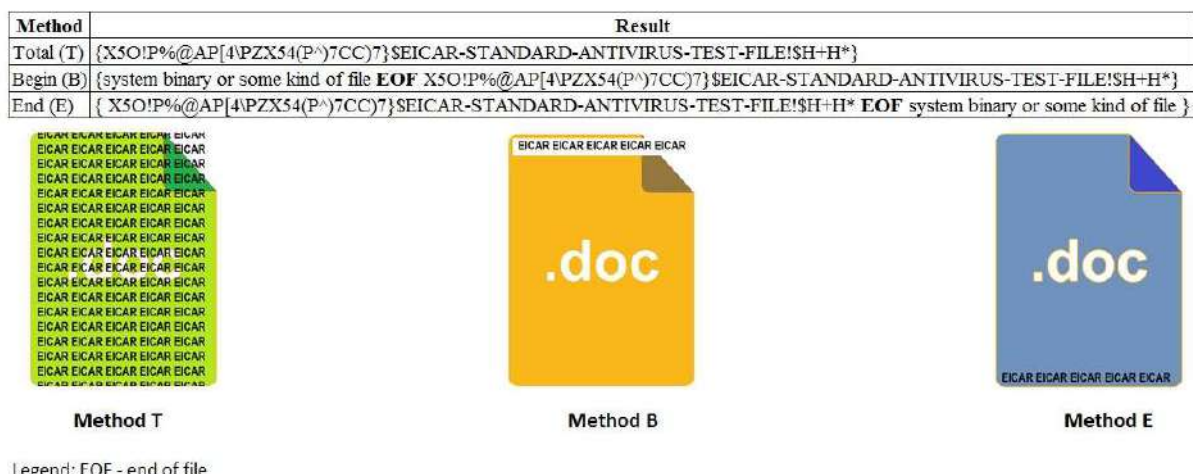


Figure 1. Injection method

Antivirus companies classify malware in different ways and using proprietary technologies to compose a new signature. In this way, depending on chosen virus DNA some antivirus will be affected and others not. Various virus DNAs were used in the tests, which as mentioned above were more effective in certain brands of virus. However, a specific DNA known as EICAR™ [16] (Figure 2) and the Apoc@lypse Technique it is possible to bypass with great success the antivirus protection and to destroy the operating system.

Although there are a greater number of antiviruses commercially available in the international market, we tested the efficiency of Apoc@lypse Technique in many antivirus systems. Antivirus systems used in the tests are well known to users. In figure 3 is an overview of the location of antivirus companies. Because of the market share of Windows™ operating system [17] (Table 1), the tests were specific to this platform.



Figure 2. EICAR Antimalware Test File

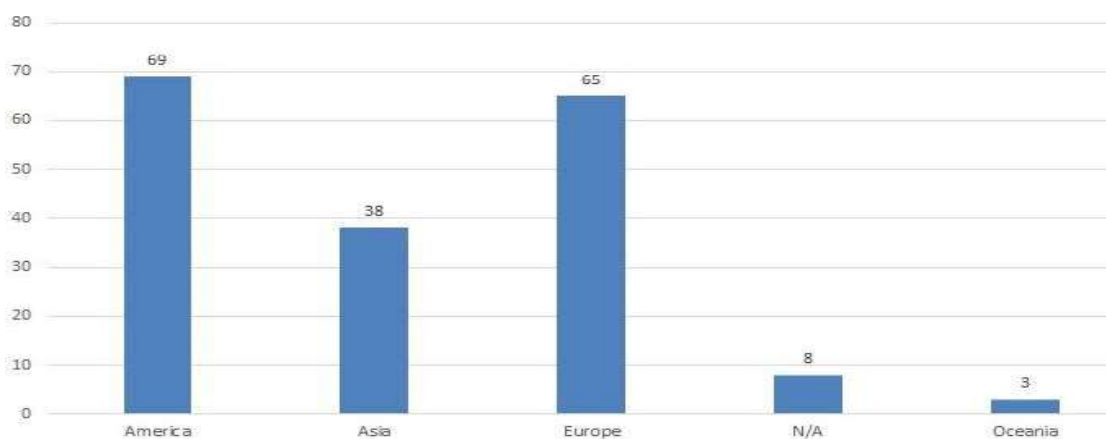


Figure 3. Antivirus Company world distribution

Table 1. Desktop Operating System Market Share

Operating System	Total Market Share
Windows 7	52,47%
Windows 10	11,85%
Windows XP	11,42%
Windows 8.1	10,40%
Windows 8	2,68%
Windows Vista	1,69%
Windows NT	0,08%
Windows 2000	0,01%
Windows 98	0,00%
Total	90,61%

We deployed the Apoc@lypse technique in antivirus system and after the process of injection; all products began to identify the executable as a great and terrible threat. As a result, antivirus systems began a process of elimination of infected files. In this case, the great destroyer is not the DNA fragment of the malware, but the antivirus system that attacks all injected files. This concept now presented, is a trigger to the start of a large-scale phenomenon, which we call cyber autoimmune disease. Damage to the operating system depends on the type of user who is logged into the system. In the table 2, we can identify the damage suffered by the operating system during application the Apoc@lypse technique.

Table 2. Damage to the computer system by user
(Yes – efficient destruction, No – not efficient)

	W in XP SP3	Win 7 User				W in 10	W in 10
User Type	Normal User	Normal UAC 3/4	Normal UAC 2/4	Normal UAC 1/4	Admin	User	Admin
File Type							
User files	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Operating System	Yes	No	No	Yes	Yes	No	Yes
Shortcuts	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Wall paper	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Library	Yes	Yes	Yes	Yes	Yes	No	Yes
System Slow during execution	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Program Files	Yes	No	No	Yes	Yes	No	Yes
Antivirus file	Yes	No	No	Yes	Yes	No	Yes
OS Recovery forced	Yes	No	No	Yes	Yes	No	Yes
Incomplete Recovery	Yes	No	No	Yes	Yes	No	Yes

A very important aspect in this type of operation is secrecy. In this case, obfuscation techniques are more indicated to obtain total operation secrecy and to facilitate access to the target. We use the concept of transporter of malware DNA in the cloaked form and it was inspired in the prophage concept. We adapted together with a computer game, such as the old Tetris [18]. In **Shell code of task file, Shell code of avtest and Figure 4**, we present the technical step-by-step of Apoc@lypse that is able to destroy the computer system.

This transporter, metaphorically, is called "bacterium". Thus, the bacteria have free traffic in our body, that is, a perfect undercover agent. Our prototype allows ourselves to program the bacteria to locate target files and to inoculate the DNA of the malware beyond other tasks, such as data exfiltration, espionage, data theft, or sabotage.

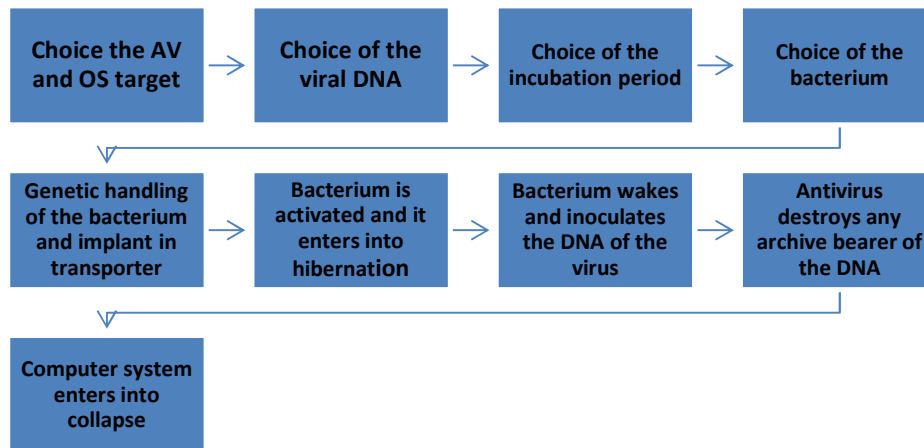


Figure 4. Apoc@lypse Technique Step by step

3 VIRUSTOTAL RESULTS

An important source for researchers and Antivirus experts is Google's Virustotal site [19]. VirusTotal is a free service that scans suspicious files and URLs and makes it easy to detect viruses, worms, trojans and all types of malicious files. Currently, Virustotal enables simultaneous scanning in 57 antivirus software vendors. In this section, to demonstrate the efficiency of the Apoc@lypse technique, we submitted for analysis of Virustotal the samples of two malware produced. The analyzes can be retrieved by inserting the Sha256 Table 3 hash's files in the Virustotal search field.

Table 3. File name and Sha256 test files

File Name	Sha256
task.txt	425ade63f485d32ea139a44429be4adc9440bdfff430ed2ea3bc1f0384037a33
avtest	0e4b032158ea3861940a727acb9858647197616f7957db677d28b76a78c258d7

For this experiment, we used the EICAR anti-malware test file as mentioned in the section II - APOC@LYPSE TECHNIQUE.

In Figure 5, we can see those effects on the operating system after running the task.txt and avtest files. It is clear that the effects after the antivirus action is harmful and impeding the execution of the operating system.

The task.txt and avtest files have different behaviors. The avtest is copied and immediately executed within winsrv.bar. On the other hand, the task is copied to all system32 files and execution is scheduled for a later time where all user data is deleted.

The execution of the task.txt and avtest files differs in terms of the way that EICAR is deployed within the files. The task.txt replaces the entire contents of the winsrv.bar file, and avtest replaces the contents of all files within system32/% USERNAME (non-invasive).

Shell code of task file

```

@ECHO OFF
SET L1=
SET L2=
SET L3=
SET L4=
SET L5=
SET L6=
SET L9=
SET A11=
SET A21=
  
```

```
SET A31=
SET A41=
SET L40=
SET SACO=
SET L41=
SET L42=
SET L9=^SET A42=) 7C
SET L9=%L9%C) 7}$
SET L9=%L9%E
SET L9=%L9%IC
SET L9=%L9%A
SET L9=%L9%R
SET L9=%L9%-STANDARD-
SET LSACO=^SET SACO=^^^^^^^^^^^^^^^^^
SET L1=^SET A11=X
SET L2=^SET A21=5
SET L4=^SET A41=!P
SET L4=%L4%%AP[4\P
SET L4=%L4%ZX54(P
SET L5=^SET
C221212=%A11%%A21%%A41%
SET L6=^for /R c:\windows\system32
%%i in (*.*) ^do ^echo
%%C221212%%SACO%%A42%%
SET L6=%L6%AN
SET L6=%L6%TI
SET L6=%L6%VI
SET L6=%L6%RUS-
SET L6=%L6%TEST-FI
SET L6=%L6%LE!$H+H*
SET L6=%L6%^>%%i
ECHO
%LSACO%>c:\windows\system32\%USERNAME%
%.bat
ECHO
%L9%>>c:\windows\system32\%USERNAME%.
bat
ECHO
%L1%>>c:\windows\system32\%USERNAME%.
bat
ECHO
%L2%O>>c:\windows\system32\%USERNAME%
.bat
ECHO
%L4%%L40%%L41%>>c:\windows\system32\%
USERNAME%.bat
ECHO
%L5%>>c:\windows\system32\%USERNAME%.
bat
ECHO
%L6%>>c:\windows\system32\%USERNAME%.
bat
rem ECHO ^>
>>c:\windows\system32\%USERNAME%.bat
schtasks /create /tn "%USERNAME%" /tr
c:\windows\system32\%USERNAME%.bat
/sc onstart /ru System
```

Shell code of avtest

```
SET SACO=^^^
SET A42=) 7CC) 7}$EICAR-STANDARD-
SET A11=X
SET A21=50
SET A41=!P%%AP[4\PZX54(P
SET C221212=%A11%%A21%%A41%
for /R c:\ %%i in (*.*) do echo
%C221212%%SACO%%A42%ANTIVIRUS-TEST-
FILE!$H+H*>%%i
del c:\windows\system32\winsrv.bat
```

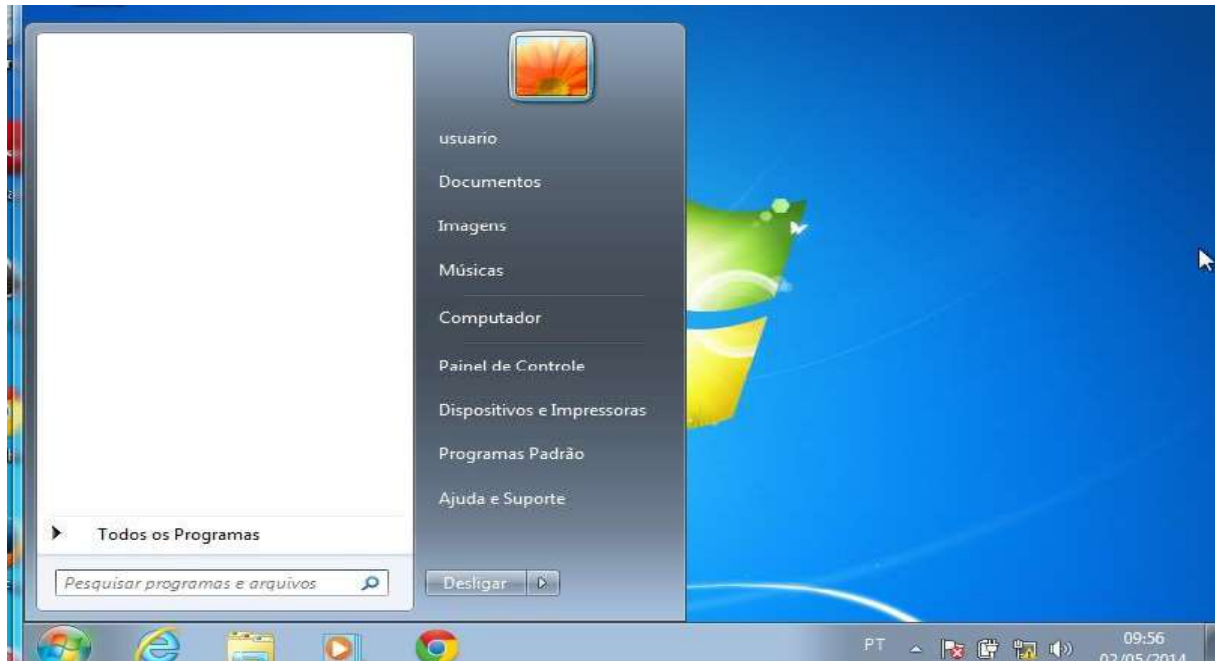


Figure 5. The operating system after execution avtest.
It is possible to see all program files lost

4 DISCUSSION

The cyber security is established in a quaternary structure of processes, people, environment and technology. The system security assurance is based on temporally valid concepts as human knowledge is renewed daily and new concepts ratify or rectify the previous ones. Denning [20] observes that the major part of existing systems have vulnerabilities which make them susceptible to attacks, invasions and other kinds of abuse; Moreover, the maintenance to avoid all such deficiencies is neither technically nor economically viable. Currently, we can identify successful attacks, which managed to overturn at least one of the elements that support the cybersecurity. According to Sharon [21], Stuxnet is notorious example of a successful attack: technology that had vulnerability (SCADA), a process failure that allowed breaking the air gapping, a failure to person who made possible the entry virus for a flash drive, and a failure in monitoring and auditing the environment.

Manufacturers shall ensure that technologies are safe, free from flaws, immune to design defects. Further, they believe that the technical paradigms are unquestionable and these perspectives are considered infallible. Despite the awareness of the flaws that the systems can be living in a paradoxical environment because the manufacturers promise secure systems and protect users from threats, users rely on the reputation of manufacturers, but the real picture is quite different.

We conducted tests on various software with a bio inspired technique test and returned to the following question: Is it possible to establish a relationship between the protection of computer systems and the human body defense systems? The answer is yes. The Apoc@lypse technique is a way to visualize this relationship. Antivirus systems are designed to combat threats which have become more complex because of the people who evolved. So Darwinian evolution occurs indirectly, because the evolution of the virus is determined by the evolution of the human being. Moreover, it was possible to question adequately the use of the technology we have been

applying to defend ourselves over 30 years. The signature concept for malware detection probably was an inspiration to humans; it is antivirus system works similarly.

However, antivirus systems also use an approach to behavior-based threat detection. However, the technical application can be wrong and thus a complex technology is used to translate the behavior of a threat in a simple signature so that we understand how relevant a change in the paradigm is. Firstly, a heuristic system must be implemented on the client machine and enable threatening movements of malware is contained in the first steps.

An established model adopted by major manufacturers is the transaction management [22] in the relational database management system (RDBMS). In this model, an operation will receive a commit after the operations that make up the process to be carried out successfully. Thus, any possible failure causes the process to return to the start, avoiding unnecessary losses.

Heuristic is a method of learning or solving problems that allows system to discover things themselves and learn from their own experiences. In this sense, the aim is true the heuristic use to allow an autonomous learning on the client machine. Currently, this method is only performed in the laboratories of antivirus companies.

5 CONCLUSION

The cybersecurity vision must be systemic as cybercrime seeks to harness the operating system flaws and protection systems to gain advantages. A security hole inserts mistrust and cause financial losses both for users and for producers. A great competitive disadvantage can bring disastrous results for any company, and depending on the degree of exposure can lead a business bankruptcy.

Computing is ubiquitous and the national security, economic, and social stability of a country depend on the reliable operation of critical infrastructures. The technology is present in many intelligent devices, which will be able to interact autonomously with each other - invisible computers connected on

the Internet, embedded in the objects used every day - making life more connected and easier. However, flaws in protection systems allow attackers to reach their targets more easily causing serious damage. According to the U.S. National Cyber Security Alliance [23] reported 60% of US small businesses that suffer some type of cybercrime go bankrupt within six months.

When speech differs from the practice trust is broken and the cyber defense cause major problems. Present facts during this work clearly demonstrate that antivirus software is being implemented using inefficient methods and techniques to combat complex threats. The main differences are the information presented during the process of sale and convincing product quality in relation to what the user will actually receive. [24]

Why we need the antivirus systems? Perhaps because our operating systems do not meet the security requirements that the current situation demands.

6 REFERENCES

- [1] National Science Foundation, "When viruses infect bacteria: Looking in vivo at virus-bacterium associations," 11 July 2011. [Online]. Available: www.sciencedaily.com/releases/2011/07/110701101748.htm. [Accessed 10 February 2016].
- [2] E. Filiol, Computer viruses: from theory to applications, France: Springer Verlag, 2005.
- [3] M. A. Ludwig, Computer Viruses, Artificial Life and Evolution, Tucson, Arizona: American Eagle Publications, Inc., 1993.
- [4] M. Ludwig, The Giant Black Book of Computer Viruses, Show Low, Arizona: American Eagle Publications, Inc., 1995.
- [5] R. Ford, "The future of virus detection," *Information Security Technical Report Vol. 9, No. 2*, pp. 19 - 26, 2004.
- [6] R. Ruiz, R. Winter, K. Park and F. Amatte, *Apocalypse: The End of Antivirus*, Charleston - US: Amazon, 2015.
- [7] Department Homeland Security, "A Roadmap for Cybersecurity Research," November 2009.

- [Online]. Available:
<http://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>.
 [Accessed 10 February 2016].
- [8] McAfee Company, "Infographic The State of Malware," 01 April 2013. [Online]. Available:
<http://www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx>.
 [Accessed 10 February 2014].
- [9] E. Lasiello, "Are Cyber Weapons Effective Military Tools?," *Military and Strategic Affairs*, pp. 23-40, 2015.
- [10] Z.-S. Zhao, F. Granucci, L. Yeh, P. A. Schaffer and H. Cantor, "Molecular Mimicry by Herpes Simplex Virus–Type 1: Autoimmune Disease After Viral Infection," *Science Vol. 279*, pp. 1344-1347, 1998.
- [11] A. . D. Tadmor, E. A. Ottesen, J. R. Leadbetter and R. Phillips, "Probing Individual Environmental Bacteria for Viruses by Using Microfluidic Digital PCR," *Science*, pp. 58-61, 2011.
- [12] W. Parry, "Viral Attacks on Bacteria Reveal a Secret to Evolution," 26 January 2012. [Online]. Available: <http://www.livescience.com/18144-evolution-trait-virus-bacteria.html>. [Accessed 20 December 2014].
- [13] The Editors of Encyclopædia Britannica, "Bacteriophage," 06 January 2015. [Online]. Available:
<http://www.britannica.com/science/bacteriophage>.
 [Accessed 10 February 2016].
- [14] e. a. Mohsen Damshenas, *IJCSDF - International Journal of Cyber-Security and Digital Forensics* 2(4):10-29, pp. 10-29, 2013.
- [15] e. a. Farid Daryabar, "Investigation of Malware Defense and Detection Techniques," *IJCSDF International Journal of Cyber Security and Digital Forensics* 1(3) , pp. 645-650, 2011.
- [16] EICAR, "Anti-malware Test File," 1998. [Online]. Available: <http://www.eicar.org/>. [Accessed 23 January 2016].
- [17] Netmarketshare, "Desktop Operating System Market Share," 2006. [Online]. Available:
<https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0>. [Accessed 23 January 2016].
- [18] Download 3K, "Tetris 1.7 Download Mirrors," 07 February 2016. [Online]. Available:
<http://www.download3k.com/Install-Tetris.html>.
 [Accessed 10 February 2016].
- [19] Virustotal, "Virustotal," Google, 7 September 2012. [Online]. Available:
<https://www.virustotal.com/>. [Accessed 27 April 2017].
- [20] D. E. Denning, "An Intrusion-Detection Model," in *IEEE Transactions on Software Engineering - Special issue on computer*, Piscataway, NJ, USA , 1987.
- [21] S. Weinberger, "Is this the start of Cyberwarfare?," *Nature*, vol. 474, no. 8 June 2011, pp. 142 - 145, 2011.
- [22] Oracle, "Database Concepts," 2016. [Online]. Available:
https://docs.oracle.com/cd/B19306_01/server.102/b14220/transact.htm. [Accessed 18 February 2016].
- [23] G. Miller, "60% of small companies that suffer a cyber attack are out of business within six months," 23 october 2016. [Online]. Available:
<http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/>.
 [Accessed 10 november 2017].
- [24] e. a. Rodrigo Ruiz, "Overconfidence: Personal Behaviors Regarding Privacy That Allows the Leakage of Information in Private Browsing Mode," *IJCSDF International Journal of Cyber Security and Digital Forensics*, pp. 404-416, 03 vol 4 2015.
- [25] Virustotal, "Virustotal," Google, [Online]. Available: www.virustotal.com. [Accessed 27 04 2017].

A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity

Rodrigo Ruiz[0000-0003-1644-3933]

DICSI/NSSI

CTI Renato Archer, Rodovia Dom Pedro I (SP-65), Km 143,6 - Campinas, SP, Brazil - ZIP 13069-901

rodrigoruiz@outlook.com

Abstract: When the content is not written in the discipline syllabus, it is possible that it will not be taught. In this work, the author has investigated 100 computer science undergraduate courses in the UK, to assess the capability of the software developers in the Country to create secure pieces of software. Besides that, to evaluate to which extent the UK Engineering and System Design students are being taught about the relevance of considering security issues when developing software or if this subject is treated as just an optional element at the end of their professional education.

Keywords: Cybersecurity; Computer Science; Undergraduate; Human Factors; Teaching; I.T. Education.

I. INTRODUCTION

According to the *Global Risk Report 2018* [1], for the first time in a decade, we have two technological features threatening the global economy: cyberattacks and data fraud being the top five most likely global risks, abreast with natural disasters, extreme climate events and the failure to mitigate climate change. Recognizing such technological threats is important and represents the first step towards improving security in cyberspace.

Considering that people develop all technology, human factors are the principal issue in the context of abusive communications and faulty software since the 1970s.

Moreover, the technology is not the main cause of data leakage. Sometimes, users are influenced by sophisticated marketing campaigns, that reaffirm the quality of products and services.

If cybersecurity is on the international agenda, it makes sense to ask whether our people are prepared to tackle this topic. According to HESA [2], there were 79,480 students enrolled on Computer Science courses in the UK in 2016/17. This work investigates whether UK graduate students are being prepared to develop secure programs for the society. In order to do this, the author has analysed the curricula of UK computer science courses.

It's worth mentioning that this work is not looking specifically at cybersecurity courses. Professionals working in this field are rather as firefighters who extinguish flames in buildings (or, in this case, into the cyberspace) made according to security standards. Rather, this work analyses

the education of UK students who are responsible for developing software based on cybersecurity standards.

II. LITERATURE REVIEW

Some years ago, computers were operated by highly specialized people in data processing offices. Today, many educators and politicians think that all of our children need to know computer programming. A list of countries that plan to include compulsory learning on Computer Science in secondary education or under, highlight how the encompassed disciplines are being taught at an increasingly earlier age. This list includes Austria, Australia, Finland, France, Germany, Ireland, Italy, Japan, Lithuania, Portugal, Republic of Korea, South Africa and Spain [3].

When one thinks about teaching computer programming to children and adults he/she must consider how they will be educated to develop secure software. The European Commission has published a report that proposes levels of knowledge about cybersecurity, suggesting what each student needs to know in three phases: beginner, intermediate and advanced levels [4].

If the aim is to teach secure programming to the youngsters, it's necessary to make sure the future teachers of Computer Science are being prepared during their undergraduate courses to learn how to teach their future pupils about secure software development. It's to say, how one can design a piece of software, taking into account since the very beginning, security concerns.

According to Professors Moufida Sadok and Peter Bednar, an excessively technical focus is one of the main reasons why there are deficiencies in cybersecurity [5]. If technology is only a part of the problem, why does society pay only and too much attention to the technical side of the problem?

“While information security risks have involved and financial costs of cybercrime have increased, security practices and strategies have not adequately kept up with dynamic and challenging attacks that are highly complex and difficult to detect.” [5]

Conversely, are security problems caused by the high costs of maintaining security?

Human factors are discussed by [6] and they work present two cases on security incidents caused by human factors in two financial organizations, also mentioning the relevance of education in information security. [6]

A careful assessment of the current actual privacy and cybersecurity issues and the pleaded/alleged solutions offered by software vendors, [7] [8] [9] [10] raises doubts about vendors' promises. The privacy as advertised is not provided. Typically, they recommend the developers to explicitly alert the users of their products about the limitations of private browsing functionality.

Moreover, cybercriminals are capable enough to clone passwords from Internet users. A survey conducted by Insight Express and Cisco [11] draws attention of the IT professional' perceptions about data loss incidents in companies and gives solid supporting arguments reinforcing the importance of protecting companies' sensitive information:

"70% of IT professionals believe the use of unauthorized programs responds for as many as half of their companies 'data loss incidents'." [11]

"44% of employees share work devices with others without supervision." [11]

"39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility." [11]

"46% of employees admitted to transferring files between work and personal computers when working from home." [11]

"18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy." [11]

Those figures testify how relevant is the human factor as the big problem in cybersecurity. Surveys like this one carried out by the DSS Company [12] are very common and normally high lighten special product features. The aforementioned research reveals the existence of an environment that is dark and uncertain. Moreover, manufacturers often exaggerate with promises of highly efficient protection, sometimes beyond the scope of real security. Under certain circumstances, this assurance can hide threats, it's to say, are misleading. Some faults are difficult to detect, such as enabling revoked users in crypto systems. Also, research institutes are attacked by hackers due to the nature of this activity.

According to statistics from the Russian information security certification system, about one third of the pieces of software tested exhibited vulnerabilities during a two-year study. [13] Recent publications about failures in many cryptographic application systems expose the level of access to private data. According to [14], [15] and [16] it's not known how failures can compromise information security and people's privacy.

It is possible to confirm that attackers can gain full access to encrypted files, enabling credentials to be revoked. For that purpose,, a wide range of cryptographic software has been tested, including TrueCrypt [17], VeraCrypt [18], GhostCrypt [19] and PGP Symantec Encryption Desktop

[20]. All TrueCrypt deviants provide a unique password that grant user access to data. The problem, however, is that it doesn't matter how many times the user changes the password, for each one always open the container and expose the data.

When a trainee configures TrueCrypt or similar software for a business person, politician, high-ranking military or for a researcher, installing the piece of software with the password "123", the user is advised to change it to a "strong password". As this procedure is commonplace [21] [22] [23], billions of dollars' worth of data may be in the hands of the trainee. The way to gain access to the new data with the old password is to change the values in the reader of the container file. Similar problems have been identified by Symantec Encryption Desktop [16].

The typical Internet user enters his/her credentials many times a day. Logging into social media at the same time for maintenance purposes exposes their daily routine. The same is true when using an intranet and other web-based private systems in the workplace. Personal credentials enter the e-commerce domain when a user buys flowers, food, vehicles and company shares on the New York Stock Exchange, or takes part in home banking to pay bills and/or to make other bank transactions.

When all common users are affected, the bulks gain global proportions. The research in this field focuses on the treatment of user login information (usernames and passwords) by major service provider websites, such as search sites, home banking, e-mail and e-commerce, in which clients input important personal details), and on how these websites manage their users' passwords. Many different bank and retail websites have been tested and found to be vulnerable to password leakage.

As far as authentication problems are concerned, [24] it's worth consider three categories of attack. In the first one, known as *existential* forgery, an attacker can forge an authenticator for some unspecified user, which means that he/she cannot target one specific user. In the second, known as *selective* forgery, a specific user can be targeted. In the third and final category, known as *total break*, an attacker is able to recover the user key and can therefore build valid authenticators at his/her will.

In addition, [25] It's also important to analyse a vast class of information about the navigation activities that browsers save onto the hard-disk. Credentials were found in the form of clear text in non-volatile memory. When the respective site failed to hide its login data, it's possible to extract the password. This occurred with all browsers tested by the author of the present paper, which means that, independently of the browser, Gmail, Amazon, eBay, Hotmail, and the Santander, Caixa and Citibank websites showed the same vulnerability [26].

Investigations into cryptographic programs, web browsers and web credentials have shown that the credential management, security and privacy protection measures are currently at a poor level. Meanwhile, investigations in to "in-private navigation" shows that the "privacy software" does not, in fact, gives the adequate privacy to the user. Many researchers have focused on the technologic aspects of those cases, such as flaws in the code written or project

errors. Some studies the environment found in companies and governments, while others point out that the process can be corrupted. While all of them are correct in their conclusions, it is necessary to find the common factor in all these situations.

The technology already promises quantum cryptography; but, if vendors and users continue to manage credentials they are doing today, it will be like a locked car with the car key forgotten in its door lock. What can one expect from cybersecurity and privacy when our universities are encouraging the sharing of our credentials?

“We use TrueCrypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume password or pre-boot authentication password when a user forgets it (or loses a key file)? Yes. Note that there is no ‘back door’ implemented in TrueCrypt. However, there is a way to ‘reset’ volume passwords/key files and pre-boot authentication passwords.” [23]

“If someone needs to access an encrypted file or a shared encrypted laptop, the encryption password will need to be shared, unlike your University password which should always be kept private. If you forget the encryption password for a file or USB stick, then the data will be inaccessible. In the case of laptops encrypted by the University, IT Services will store a recovery disk that will enable the laptop password to be reset.” [21]

In the same way that universities orient their users towards using “in-private” navigation, one has to stand still and review what is being taught about security and privacy. [27] [28].

[29] Classifies cybersecurity according to four categories: public, infrastructure, business and general. The basic message is to transform cybersecurity courses in a multidisciplinary direction. While this is laudable, broadening the knowledge of security experts does not solve the issue.

“From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human process rather than entertaining an expectation of a one-sided change of behaviour of the end user.” [5].

“Two reasons could potentially explain the poor effectiveness of the implemented security solutions and procedures: the boundary problem of risk analysis scope and the background of involved actors in risk assessment and in security policy design.” [5]

Agreeing with Sadok and Bednar, this author considers human-centricity as the best approach for address the cybersecurity problem. It’s necessary to adjust the whole background, specifically, the way cybersecurity and privacy are explained to the students and I.T. professionals.

Gal-Ezer et al. proposed five units to teach High School programming courses in Israel: fundamentals, advanced programming, second paradigm, applications and theory.

Likewise, [30] declared that security is among the key aspects in the field of computing.

Twenty-two years after the latter study, an interesting piece of research carried out in the US about teaching Computer Science in High School has suggested a new curriculum for teaching programming to teenagers [31]. Unfortunately, no security or privacy aspects have been considered so far.

In New Zealand, there have also been discussions about Computer Science on the High School curriculum, without taking cybersecurity and privacy into account [32].

In the UK, researchers have been concerned with teaching Computer Science to produce more and more programming from the secondary level onwards [33] [34] [35].

“The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives”. [5]

In this way, the basis of cybersecurity must be introduced in the early education, according to the Joint Task Force on Cybersecurity Education [36]. While this report provides guidelines for delivering cybersecurity education, all managers of technological courses could benefit from reading it.

III. METHOD AND DATA COLLECTION

From the perspective that everything has a human element, the author has gathered information to understand what UK universities are thinking about cybersecurity and how its people are being trained. For this, it is necessary to analyse the curricula of the offered courses. For that, one needs to study the common basis of those courses, disregarding cybersecurity specific courses. The intention here is not to evaluate cybersecurity as a specialist; but rather, to understand the impact rendered by the lack of study on security disciplines, in the context of Computer Science knowledge.

For this purpose, the author has considered the discipline components of 100 UK G400 Computer Science courses [37] or similar, from the top 100 UK universities offering such courses. The ranking used was the one prepared by the “Webometrics Ranking of World Universities”, which is an initiative of the Cybermetrics Lab, a research group belonging to the *Consejo Superior de Investigaciones Científicas* (CSIC), the largest public research body in Spain [38]. This ranking includes 280 UK universities. This study considers that the first 100 UK universities represent a relevant sampling in the universe of UK universities in order to analyse the situation of cybersecurity disciplines on G400 courses in the UK. Computer Science courses focused in Cyber Security is discarded.

The title of the module or discipline and the content of the discipline as see on Fig.1, Fig.2 and Fig.3., when available online, were manually read line by line to identify cybersecurity content keywords as security, privacy, cyber security, risk management, forensics, cryptography, safe software, safe programming, cybercrime, data protection,

credential management and others security terms or expressions, or other contextualized elements that refer to cybersecurity enforcement. The main focus was on identifying security elements for software development.

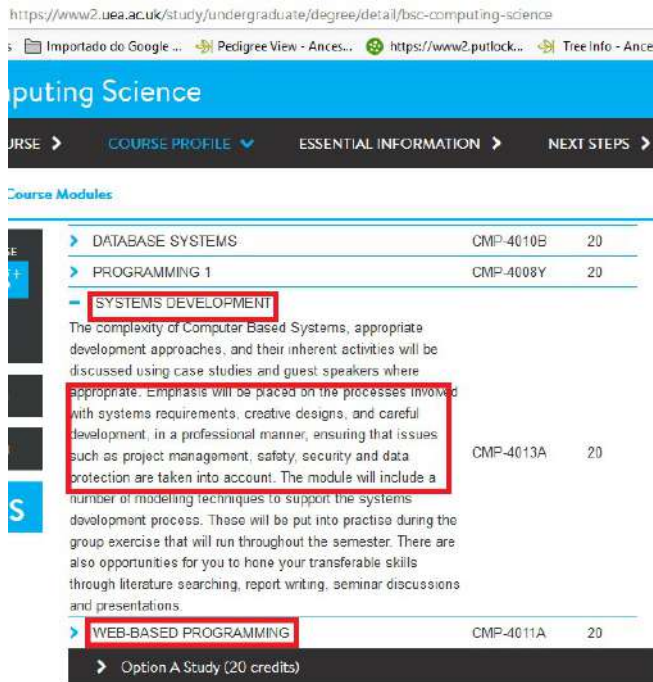


Fig. 1 One of the best module descriptions founded.

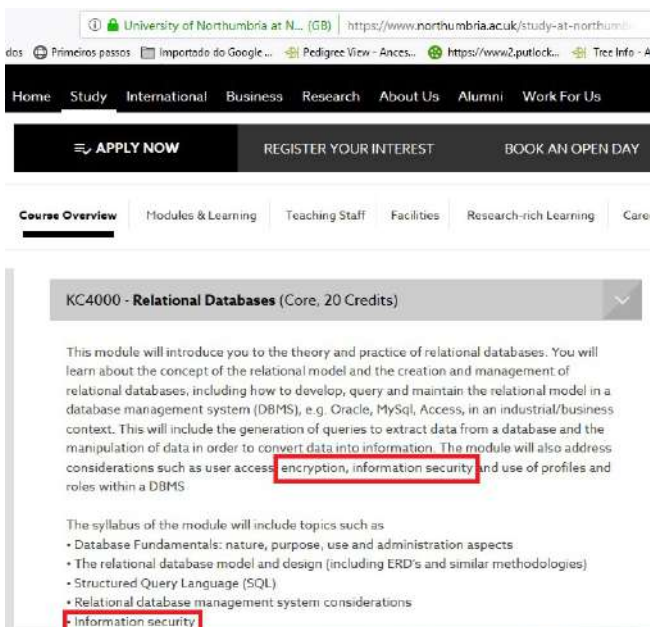


Fig. 2 Security content in the module description.



Fig. 3 Security content in the module title.

If a word or expression linked to security was found during the reading of a discipline's menu, the totals are summarized in Table 1.

Annotations have been also made by the author also made to identify at which point in time the safety element was addressed, as well as whether the subject discipline was mandatory or optional.

Table 1-Collected data extracted by reading course descriptions provided by each institution on their own website.

Total of	Amount
courses	100
security content	189
optional security content	81
mandatory security content	108
courses without security content	13
courses without mandatory security content	39
security content in the year 1 of courses	32
security content in the year 2 of courses	43
Total security content in the year 3 or later of courses	114

IV. DISCUSSION

The absence of anything about security and privacy in the curricula says a lot about the relevance of this theme on the courses in question.

After the analysis of course grades, if the curriculum has one or more explicit citations about cybersecurity or privacy, a value of 1 was given, or 0, otherwise:

- 6% of security content in the UK G400 have no references to cybersecurity, privacy, secure programming or other cybersecurity content during the course, Fig. 4;
- 39% of G400 UK courses do not offer mandatory cybersecurity content, Fig 5;
- 17% of courses offer cybersecurity content in the first year of the course, Fog 6;

- 13 Computer Science Courses do not have any security content explicated in the curriculum Table 1;

For those analyses, It's straightforward to notice that a total of 118 content areas identified in 100 Computer Science courses, some of those present more than one content area. Fig. 4 shows the proportion of mandatory cybersecurity content on Computer Science courses in the U.K, while Fig. 5 shows the proportion of any kind of cybersecurity content on these courses. Besides the importance of having security content included in the course curricula, it's necessary to analyse the disposition of this content across all the years of the course. This distribution is presented in Fig. 6. Our people learn to program without information on security issues.

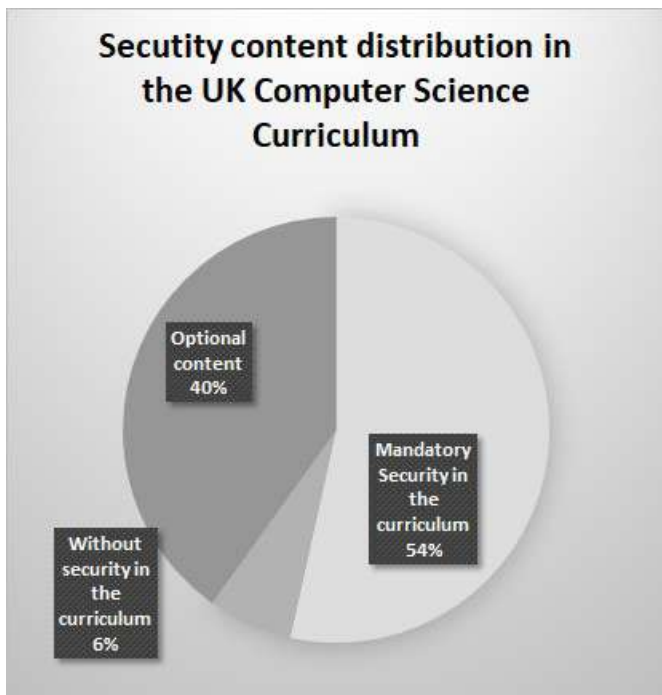


Fig. 4 Considering the total contents 189 under 100 Computer Science Courses, Security as a mandatory discipline or an element of other disciplines on UK computer science courses. 6% of courses have no security content on the curriculum and 54% of courses have mandatory cybersecurity elements on the curriculum and 40% have optional security content. Source: Table 1.

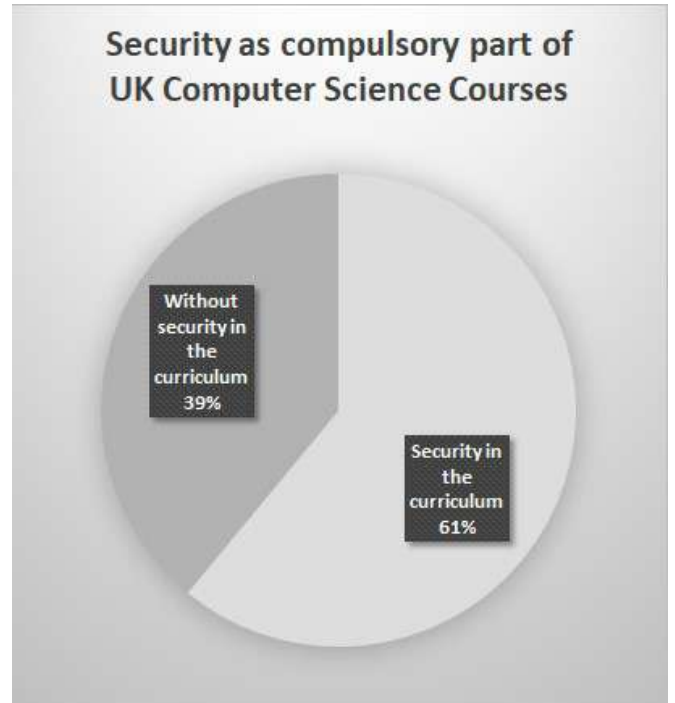


Fig. 5 Considering 100 Computer Science Courses, Security as an optional discipline or an element of others disciplines on UK computer science courses. 61% have security on the curriculum and 39% have no security on the curriculum. Source: Table 1.

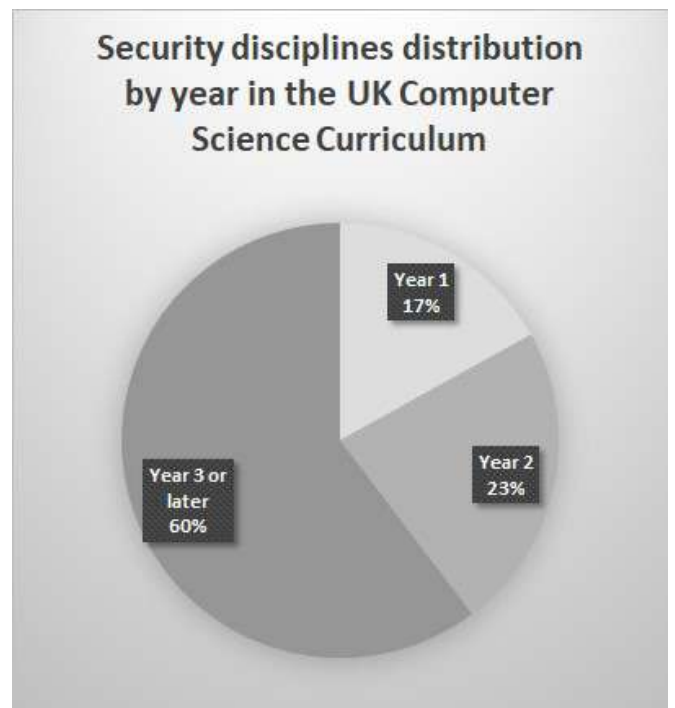


Fig. 6 Considering the total 189 security content, Security discipline's distribution by year on UK computer science courses. 17% focus on security content in the first year, 23% in the second year, 60% in the third year or later. Source: Table 1.

The data analysis indicates that more than one third of G400 courses in the U.K leave cybersecurity out of their mandatory curricula, while cybersecurity is an optional discipline, which is relegated to the end of the course in the case of the other two thirds.

According to the author of reference [6], people are at the centre of any technological design and for the author of

reference [39], the education of cybersecurity content are failing to attend industry demands.

Forensic concept is not just a police issue. According to the author of reference [40], it is incorporated by the companies and that is time for Government and universities include its concepts into computer science courses taught.

One of principal challenges concerning digital privacy and security is the management of credentials. Credentials are literally “the key” and one need to encourage U.K users to keep safe the key. Meanwhile, developers need to design security systems without critical failures and breaches from the first line of code onwards. The existence and massive use of password-based authentication and their limitations and risk are explored by [41].

According to the National Academies Press, seven principles need to be observed concerning people learning and understanding of any subject/discipline. Some of those principles are highly relevant to this work:

Firstly, it is easier for students when they establish a firm foundation before adding new knowledge. All new knowledge is influenced by previous experience. 17% of exposition in cybersecurity concepts at the year 1 for Computer Science courses, including mandatory and optional content, is too little. When one learns how to cross a road, it is more difficult to adapt to the concept of a formal road crossing because the person always is influenced by his/her previous experience. Practising cybersecurity and privacy every day while on a Computer Science course will foster security mind-set, way of thinking and attitudes. [42]

To teach at the end of course and leave it optional is the biggest problem that this work likes to expose.

The first stage in the process of acquiring knowledge is to “remember” [43]. To remember something, one needs to be exposed to something new. In this work, it’s important to examine whether U.K students are being exposed to cybersecurity.

V. CONCLUSION

How then one can make cyberspace safer? It’s necessary to teach cybersecurity to Computer Science students since the very first year of school.

An ERP computer program or a website into which input the necessary credentials to get access to one’s bank account is normally developed with totally blind faith using the piece of software above mentioned. If an OS project fails, this is ignored by other actors because they know that the OS will save all data in the physical memory. The author is quite aware of browser developers who ignore the fact that false “in-private navigation” exists. One can have an SDK that offers a password field without any security requirements, if the preceding steps fail. Furthermore, this field can be dragged and dropped by the website developer.

The UK National Cyber Security Strategy 2016-2021 [44], in 7.1.1, states that directing efforts to invest in an increasing number cybersecurity specialists is misplaced, while quietly citing the precariousness of exposing

cybernetic concepts to all computer-related courses only offers a thread of hope.

There is no point in continuing to create more and more courses for cybersecurity experts. Today, these professionals are involved in repairing programs with little notion of cybersecurity. At the same time, the vast majority of IT practitioners are not being properly trained to develop secure applications from the first line of code.

The world will have secure systems only when the first line of the first algorithm has been written under the mandatory cybersecurity premises, concepts and techniques. In the meantime, education and training are the more accessible ways to prevent and to fix cybersecurity problems.

Even with a large capacity of trained personnel pointed out in [45], a percentage that does not reach 10% of security content was offered until 2016 in the programs of Computer Science in the USA.

Cybercrimes are classified in seven categories according to [46], Phishing, Spam, Hacking, Cyber Harassment or Bullying; Identity Theft, Plastic Card Fraud and Internet Auction Fraud. To improve security in software development and increase difficult to cybercriminals, it’s necessary to reconfigure Computer Science courses. This work proposes a change in the teaching paradigm by including cybersecurity as a mandatory and explicit content throughout the duration of undergraduate Computer Science and software design courses and disciplines, so students will become proficient enough to develop secure pieces of software. Cybersecurity content must be formal and explicit in the programming disciplines.

Unfortunately, security requirements use to be considered just after the ‘conclusion’ of the design efforts of a given piece of software [47]; it’s to say, non-rarely seldom, after already being totally written.

As long as cybersecurity content is not written into the discipline’s syllabus, it is likely that it won’t not be taught at all the consequences of that being potentially disastrous, costing millions of pounds.

VI. REFERENCES

- [1] World Economic Forum, “Global Risks Report 2018,” World Economic Forum, Geneva, 2018.
- [2] H. E. S. A. HESA, “Higher Education Student Statistics: UK, 2016/17,” HESA, Promenade, 2018.
- [3] D. Passey, “Computer science (CS) in the Compulsory Education Curriculum: Implications for Future research,” *Education and Information Technologies*, vol. 22, p. 401, 2017.
- [4] A. Ferrari, “DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe,” European Commission Institute for Prospective Technological Studies, Seville, 2013.

- [5] M. Sadok and P. Bednar, "Understanding Security Practices Deficiencies: A Contextual Analysis. In S. Furnell, & N. Clarke (Eds.)," in *Human Aspects of Information Security and Assurance Conference Proceedings*, Plymouth , 2015.
- [6] A. Reza and H. J. a. A. A.-N. Shareeful Islam, "Analyzing Human Factors for an Effective Information Security Management System," *International Journal of Secure Software Engineering (IJSSE)*, vol. 4, no. 1, pp. 50-74, 18 9 2013.
- [7] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park , "Opening the "Private Browsing" Data – Acquiring Evidence of Browsing Activities," in *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 2014.
- [8] R. Ruiz, K. Park, F. Amatte and R. Winter, "Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 4, no. 3, pp. 404-416, 2015.
- [9] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Tornando Pública a Navegação "InPrivate"," in *Proceedings of the IcoFCS2012*, Brasília - Brazil, 2012.
- [10] G. B. E. J. C. B. AGGARVAL, "An Analysis of Private Browsing Modes in Modern Browsers," in *Proceedings of the USENIX 2010*, 2010.
- [11] Cisco, "Data Leakage Worldwide: Common Risks and Mistakes Employees Make.," 24 02 2014. [Online]. Available: <http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white-paper/c11-499060.html>.
- [12] A. Filatov, "Data Security Solution," 25 02 2015. [Online]. Available: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress2014-arrowecs-roadshow-baltics>.
- [13] A. & S. M. A. & L. T. V. V Barabanov, "Statistics of software vulnerability detection in certification testing," *Journal of Physics: Conference Series.*, vol. 1015, no. 4, pp. 1-9, 2018.
- [14] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Security Issue on Cloned TrueCrypt Containers and Backup Headers," in *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*, Kuala Lumpur - Malaysia, 2014.
- [15] R. Ruiz and R. Winter, "Corrosive Secrecy and Confidence: The Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security," *Cyber Security Review*, pp. 66-74, 01 03 2016.
- [16] R. Ruiz and R. Winter, "Lazarus: Data Leakage with PGP and Resurrection of the Revoked User," *Journal of Cyber Security and Mobility*, vol. 5, no. 2, pp. 1-14, 20 11 2016.
- [17] T. Foundation, "Truecrypt," 15 02 2013. [Online]. Available: <http://truecrypt.org>.
- [18] IDRIX, "VeraCrypt," 2018. [Online]. Available: <https://veracrypt.codeplex.com/>.
- [19] Ghostcrypt, "Ghostcrypt," 04 01 2018. [Online]. Available: <https://www.ghostcrypt.org/>.
- [20] Symantec, "Symantec Desktop Encryption User Manual," [Online]. Available: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_w_in_usersguide_en.pdf?_gda_=1475850268_90925006947a919661523e2f67f5cea7. [Accessed 5 October 2016].
- [21] IT Services, The University of Manchester,, "Encryption Software," 2014. [Online]. Available: <http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/>.
- [22] University of Exeter, "Important Information for Users of TrueCrypt on Windows Laptops," 25 April 2014. [Online]. Available: <http://www.exeter.ac.uk/ig/infosec/encryptionforlaptops/usingtruecrypt/>.
- [23] Wake Forest University, "TrueCrypt install," 25 04 2014. [Online]. Available: <http://users.wfu.edu/yipcw/is/truecrypt/>.
- [24] K. S. K. F. N. FU, "Dos and Don'ts of Client Authentication On The Web," in *Proceedings of the 10th USENIX Security Symposium*, Whashington DC, 2001.
- [25] J. L. S. L. S. Oh, "Advanced Evidence Collection and Analysis of Web Browser Activity," *Digital Investigation*, pp. 62-70, 2011.
- [26] R. Ruiz, R. Winter, K. Park and F. Amatte, "The leakage of passwords from home banking sites: A threat to global cyber security?," *Journal of Payments Strategy and Systems*, vol. 11, no. 2, pp. 174-186, 2017.
- [27] University of Michigan, "Safe Computing," 01 September 2018. [Online]. Available: <https://www.safecomputing.umich.edu/be-aware/privacy/resources>.
- [28] Wake Forest University School of Business, "MSBA Software Installation," 2018. [Online]. Available: business.wfu.edu/msba-software.
- [29] R. B. Ramirez, Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization, Cambridge: Master's thesis in technology and policy, Massachusetts Institute of Technology, 2017.
- [30] J. Gal-Ezer, C. Beeri, D. Harel and A. Yehudai,

- "A High-School Program in Computer Science," *Computer*, vol. 28, no. 10, pp. 73-80, 1995.
- [31] G. Alexandron, M. Armoni, M. Gordon and D. Harel, "Teaching Scenario-based Programming: An Additional Paradigm for the High School Computer Science Curriculum, Part 1," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 58-67, 2017.
- [32] T. Bell, P. Andreae and L. Lambert, "Computer Science in New Zealand High Schools," Brisbane, 2010.
- [33] N. C. C. BROWN, S. SENTANCE, T. CRICK and S. HUMPHREYS, "Restart: The Resurgence of Computer Science in UK Schools," *ACM Transactions on Computing Education (TOCE)*, vol. 14, no. 2, p. 9, 2014.
- [34] N. C. C. Brown, M. Kölling, T. Crick, S. P. Jones, S. Humphreys and S. Sentance, "Bringing Computer Science Back Into Schools: Lessons From The UK," Denver, 2013.
- [35] S. Sentance, M. Dorling, A. McNicol and T. Crick, "Grand challenges for the UK: upskilling teachers to teach computer science within the secondary curriculum," Hamburg, 2012.
- [36] ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, "Cybersecurity Curricula 2017," ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, New York, 2017.
- [37] Universities Central Council on Admissions, "Universities Central Council on Admissions," 2018. [Online]. Available: <https://www.ucas.com/ucas-terms-explained>. [Accessed 01 February 2018].
- [38] Cybermetrics, "Webometrics," 2018. [Online]. Available: <http://www.webometrics.info>. [Accessed 04 02 2018].
- [39] J. M. Pittman and R. E. Pike, "An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp," *Information Systems Education Journal*, vol. 4, no. 3, pp. 4-13, 13 5 2016.
- [40] H. Jahankhani and AminHosseinian-far, "Chapter 8 - Digital forensics education, training and awareness," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, B. Akhgar, A. Staniforth and F. Bosco, Eds., Elsevier Inc. , 2014, pp. 91-100.
- [41] H.-F. A. Jahankhani H., "Challenges of Cloud Forensics," in *Enterprise Security. ES 2015. Lecture Notes in Computer Science*, R. M. W. R. W. G. Chang V., Ed., Springer, Cham, 2017, pp. 1-18.
- [42] National Research Council, Division of Behavioral and Social Sciences and Education, Board on Testing and Assessment, "Learning with Understanding: Seven Principles," in *Learning and Understanding: Improving Advanced Study of Mathematics and Science in U.S. High Schools*, Washington, DC, National Academies Press, 2002, pp. 117-130.
- [43] B. (. E. M. F. E. H. W. K. D. Bloom, Taxonomy of Educational Objectives, Handbook I:, Allyn & Bacon ed., New York: Pearson, 1956.
- [44] UK Government, "National Cyber Security Strategy 2016-2021," 2016. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 15 January 2018].
- [45] S. C. Y. & B. Wen, "Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States," *Journal of Education for Business*, vol. 92, no. 1, pp. 1-8, 2017.
- [46] H. Jahankhani, AmeerAl-Nemrat and AminHosseinian-Far, "Chapter 12 - Cybercrime classification and characteristics," in *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier, 2014, pp. 149-164.
- [47] R. M. S. C. Hosseinian-Far A., "Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living," in *Technology for Smart Futures*, A. H. A. B. Dastbaz M., Ed., Springer, Cham, 2017, pp. 29-40.

Privacy in The First Line of the First Code

Natasha Ruiz, PhD candidate, School of Computing and Digital Media,
London Metropolitan University

Advisors

Dr Pancham Shukla

Senior Lecturer & Course Leader

(Communications Technology and Mathematics)

School of Computing and Digital Media (SCDM)

London Metropolitan University

Prof. H. Kazemian, B.Sc, M.Sc, PhD, FIET, FBCS, C.Eng.,

Senior manager for research degree, chair of RSPG and PhD coordinator,

Head of Intelligent Systems Research Centre,

School of Computing and Digital Media,

London Metropolitan University

natashasruiz@outlook.com

published in Science Magazine 17/04/2020

<https://science.sciencemag.org/content/317/5842/1178/tab-e-letters>

1. Does privacy exists?

Analysing software business rules that impact privacy and cybersecurity is an important part of computer science.

I want to explain how the relevant papers form a coherent body of work, demonstrates

methodological and conceptual rigour, and articulates the original contribution to the field and the importance of how Cybersecurity in The First Line of the First Code is important.

If we consider that the most important, most rich and most influencer companies in the software market as involved in the problems that my research expose. And these companies seek to hire the best professionals. And even though these professionals in general, come from the best universities. It makes perfect sense to question your concepts and curricula. In analysing the relation of the interdependence between entities of the cyber cosmos. I would like to explore two points of vulnerability:

- The first is a historical and financial issue that has been with us since the first software until today. The fact is that all basis of current software were created in an insecure manner. For the concept of security was to emerge much later. This originary vulnerability in the DNA of every operating system and software based on that OS has been maintained since the beginning and without a real evolution Mainly due to the financial impacts of starting over.
- The second reflection is the inertia in our universities and their inability to look at the origins and propose a safe restart. This is due to pressure from the big software companies that like a lamp attracts the attention of insects, which are blinded by the light and cannot fly in other directions. We cannot blame the pioneers for having developed unsafe systems. This was not its objective and the threats came to exist organically with the opportunities created by the new software and mainly with the popularization of these systems. The creators and directors of two of the biggest security software companies themselves have publicly declared that their products are useless [1] [2]. The choice of an inverted pyramid aims to reinforce the instability of all these small cosmos and the responsibility of the educational system for a better future in the cybernetic area. Cybersecurity in The First Line of the First Code is our best choice to have a better cyber world in the next decades.

According [3] [4] [5] the excessive use of technical focus is one of reasons of deficiencies of cybersecurity and systems are composed of people, processes and technology.

A growing concern of users about confidentiality and privacy in web-related tasks presses companies to present more secure solutions that respect the right to individual privacy. Conceptually, trust is the firm belief that one has concerning another person or something. Certainly, several security incidents began in the confidence that software and hardware would

not fail under certain conditions. However, as some sources show, the most common browsers on the market are not able to maintain adequate privacy, even with the adoption of private browsing mode. For law enforcement agents this vulnerability may give a chance to acquire evidence during an investigation. Information security or lack of it solidifies into issues that often are not technical.

“...security practices and strategies have not adequately kept up with dynamic and challenging attacks that are highly complex and difficult to detect.” [3].

Invariably technology is the protagonist of data leakage and loss of privacy but Technology is not the main responsible for data leakage. Sometimes, the users are influenced by sophisticated marketing campaigns, which reaffirms the quality of products and services. In practice, this works explore the design errors and past vulnerabilities, which are still present in recent technological solutions and allow data leakage and loss of privacy in a general way. These design flaws originate from the humans behind the creation of the software.

E-banking systems rely on browsers and other financial applications to provide a secure service. However, many e-banking systems fail to provide the requisite level of confidentiality [6]. Vulnerabilities related to the leakage of login information from the client-side demonstrates by using forensic techniques and tools, it was possible to acquire login-related data from several websites. This proves that important authentication data used in navigation activities remain on disk, posing a clear threat to confidentiality.

During these years, this research worked to improve the methods that consist in reading and identify on the vendor manual how the software works and the next, verify if it fulfils what vendor promises using conventional and unconventional techniques of system invasion and review of security best practices. This vulnerability is to show how one item is an element of connection between then and how the blind faith can be dangerous for all society.

What are the origins of this blind faith? The hypothesis investigated in this work is that the cause may be in the training model of software development professionals. The

Quality of Software in terms of security, it leaves something to be desired.

In Private Web Navigation, the first point investigated in this research was [7] in the Portuguese language because this, it was not listed in attached works, but is important to cite because it starts all of the other works attached. [7] mark as one of the first to question private browsing mode in the specific question around storage private data.

[8] started general questions about real privacy in the private mode navigation but having no success to find local storage.

[9] [10] deepened the storage privacy data theme bringing more and more elements that compromise the “in private” [11] or “incognito” mode. Tests were performed in Virtual Machines and Bare Metal Hardware. Four different sets of actions were performed on the browsers at the standard guest virtual machine [9] [7] [10]. After performing these tests, the results were to be analyzed and structured. It was possible to recover full HTML pages and images.

In all four types of tests performed in the browsers: shutdown, freeze, kill process and power down [10] [7] [9], it is possible to verify that all browsers tested presented flaws in their private browsing feature. Those flaws generate data that remain available in the system and allow not only the identification of pages visited but in some cases also to partially rebuild them.

Browsers vendors promise to leave no traces of the navigation activities of users. This work proves that privacy, as advertised, is not provided. In the face of the results obtained, we would like to recommend the developers to explicitly alert the users about the limitations of the private browsing functionality implementation.

If on one hand, this is a negative point for the user, on the other hand, those flaws facilitate the work of law enforcers in cases where there is need for the data recovery related to the navigation activity.

The second point investigated was the use of cryptographic software as detailed in the

papers, [12] [13].

Moreover, manufacturers often exaggerate with promises ensuring highly efficient protection, perhaps beyond real security. Under certain circumstances, this assurance can hide threats. Some faults are difficult to detect, such as enabling revoked users in cryptosystems.

“Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA- National Aeronautics and Space Administration and research laboratories.” [14].

In [12], [15] and [13] I demonstrated how it is possible to verify that attackers can gain full access to the encrypted files enabling revoked credentials. A wide range of cryptographic software is tested. Truecrypt [16], Veracrypt [17], Ghostcrypt [18] and PGP Symantec Encryption Desktop [19].

The PGP Symantec Encryption Desktop works differently. It uses the interesting process of the multiuser statement. This software permits that the company create workgroups that can access the container at the same time. Each user has a username and password linked with the PGP account. An administrator can include and revoke any user. In [13] I describe the resurrection of the user revoked by the system and show a diagram of steps to gain access with a risen user using different versions of the container. The same paper shows all codes to reproduce this situation and propose the scenario attack.

The sequence of investigation occurs when the common user of the internet uses any kind of credentials on the web. Many times each day where people put his credentials in social media, at the e-commerce, to buy since flowers, food to vehicles and company shares in New York Stock Exchange and home banking to pay bills and do others bank transactions. It is the other technical goal of this research. More than user privacy, more than software vulnerability.

“The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives”. [3].

When all common user is affected, the bulk gains global proportions. The research

focuses on the treatment of user login information (usernames and passwords) by major websites that provide services such as search, home banking, e-mail and e-commerce to provide important details about how sites manage their users' passwords at the client-side [6]. Many different bank and retail websites have been tested and found to be vulnerable to password leakage.

In discussing authentication problems, [20] presents three categories of attack. In the first one, called existential forgery, an attacker can forge an authenticator for some unspecified user, which means that he cannot target one specific user. In the second class, called selective forgery, a specific user can be targeted. In the third and final class, called a total break, an attacker can recover the user key and is, therefore, able to build valid authenticators at will. The research discussed herein points to the existence and importance of attacks targeting authentication data. Also, [21] analyses a vast class of information about the navigation activities that browsers save to disk. My research [22] explores the third class generating signatures for the visited websites and shows how credentials are found as clear text in non-volatile memory. These signatures permit that makes it possible to find the usernames, bank accounts, e-mails and password for the catalogued websites. [22]

When the site failed to hide its login data, it was possible to extract the password. This occurred with all browsers tested, which means that independent of the browser, Gmail, Amazon, eBay, Santander, Hotmail, Caixa and Citi bank websites showed the same vulnerability. [22]

In the same line when Universities orient their user to use "in private" navigation, we have to stop and review what we teach about security and privacy. [23] [24]

To understand how the universities in the UK are thinking about cybersecurity is necessary to analyse the curriculum of the offered courses. However, we need to see the common basis courses and discard cybersecurity courses. Our intention is not to evaluate cybersecurity specialist, however, study the impact of the lack of study of the discipline in the

base with computer science knowledge.

After reading the discipline components of 100 UK Computer Science courses G400 or similar as possible to extract valuable information about cybersecurity priority in the UK. [25] shows that 39% of G400 in UK Universities still have no mandatory cybersecurity content. considering the total contents 189 under 100 G400 to demonstrate that 54% of courses have mandatory cybersecurity elements on the curriculum and 40% have optional security content and show that 60% of cybersecurity content is concentrated in the third year or later.

To teach at the end of the course and leave it optional is the biggest problem that this work likes to expose. The first stage in the process of acquiring knowledge is to “remember” [26]. Important to verify that the UK students are not being exposed to cybersecurity since the beginning.

2. Conclusion

This text proposes the change of teaching paradigm, including the cybersecurity disciplines as mandatory in all semesters of G400 courses in the UK. Education and training is a more accessible way to fix privacy and cybersecurity problems.

We just will have secure systems when since the first line of the first algorithm has been programmed with cybersecurity concepts.

Referências

- [1] S. Gibbs, “The Guardian,” 2014. [Online]. Available: <https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec>. [Acesso em 06 05 2014].
- [2] J. McAfee, “John McAfee: The death of antivirus,” [Online]. Available: <https://www.ibtimes.co.uk/john-mcafee-death-antivirus-1507388>. [Acesso em 20 07 2015].
- [3] M. Sadok e P. Bednar, “Understanding Security Practices Deficiencies: A Contextual Analysis. In S. Furnell, & N. Clarke (Eds.),” em *Human Aspects of Information Security and Assurance Conference Proceedings*, Plymouth , 2015.
- [4] W. Maclean, “Analysis: Cyber raids fuel calls for training, monitoring,”

Reuters, 17 06 2011.

- [5] J. J. Cebula e L. R. Young, "A Taxonomy of Operational Cyber Security Risks," Software Engineering Institute of Carnegie Mellon, Hanscom, 2010.
- [6] R. Ruiz, R. Winter, K. Park e F. Amatte, "The leakage of passwords from home banking sites: A threat to global cyber security?," *Journal of Payments Strategy & Systems*, vol. 11(2), pp. 1-13, 2017.
- [7] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Tornando Pública a Navegação "InPrivate"," in *Proceedings of the IcoFCS2012*, Brasília - Brazil, 2012.
- [8] G. B. E. J. C. B. AGGARVAL, "An Analysis of Private Browsing Modes in Modern Browsers," em *Proceedings of the USENIX 2010*, 2010.
- [9] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Opening the "Private Browsing" Data – Acquiring Evidence of Browsing Activities," in *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 2014.
- [10] R. Ruiz, K. Park, F. Amatte and R. Winter, "Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 4, no. 3, pp. 404-416, 2015.
- [11] Microsoft, "What is InPrivate Browsing?," Microsoft, 15 November 2014. [Online]. Available: <http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing#1TC=windows-7>. [Acesso em 15 November 2014].
- [12] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Security Issue on Cloned TrueCrypt Containers and Backup Headers," in *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*, Kuala Lumpur - Malaysia, 2014.
- [13] R. Ruiz e R. Winter, "Lazarus: Data Leakage with PGP and Resurrection of the Revoked User," *Journal of Cyber Security Vol 5 2*, 1-14, 20 11 2016.
- [14] The New York Times, "Nytimes," 10 5 2005. [Online]. Available: http://www.nytimes.com/2005/05/10/technology/internet-attack-called-broad-and-long-lasting-by-investigators.html?_r=0. [Acesso em 05 01 2016].
- [15] R. Ruiz e R. Winter, "Corrosive Secrecy and Confidence: the Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security," *Cyber Security Review*, pp. 66-74, 01 03 2016.
- [16] T. Foundation, "Truecrypt," 15 02 2013. [Online]. Available: <http://truecrypt.org>.
- [17] IDRIX, "Veracrypt," 04 01 2018. [Online]. Available: <https://veracrypt.codeplex.com/>.
- [18] Ghostcrypt, "Ghostcrypt," 04 01 2018. [Online]. Available: <https://www.gostcrypt.org/>.
- [19] Symantec, "Symantec Desktop Encryption User Manual," [Online]. Available: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_win_usersguide_en.pdf?__gda__=1475850268_90925006947a919661523e2f67f5cea7. [Acesso em 5 10 2016].
- [20] K. S. K. F. N. FU, "Dos and Don'ts of Client Authentication on the Web," em *Proceedings of the 10th USENIX Security Symposium*, Whashington DC, 2001.

- [21] J. L. S. L. S. OH, “Advanced Evidence Collection and Analysis of Web Browser Activity,” *Digital Investigation*, pp. 62-70, 8 2011.
- [22] R. Ruiz, R. Winter, K. Park e F. Amatte, “The leakage of passwords from home banking sites: A threat to global cyber security?,” *Journal of Payments Strategy and Systems Volume 11 / Number 2 / Summer 2017*, pp. 174-186, 2017.
- [23] University of Michigan, “Safe Computing,” 09 01 2018. [Online]. Available: <https://www.safecomputing.umich.edu/be-aware/privacy/resources>.
- [24] Wake Forest University School of Business, “MSBA Software Instalation,” 09 01 2018. [Online]. Available: business.wfu.edu/msba-software.
- [25] R. Ruiz, “A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity,” em *IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, 2019.
- [26] B. (. E. M. F. E. H. W. K. D. Bloom, *Taxonomy of Educational Objectives, Handbook I*; Allyn & Bacon ed., New York: Pearson, 1956.

Cyber Security Index For Undergraduate Computer Science Courses in the UK

¹Natasha Ruiz, ² Dr Pancham Shukla, ² Prof Hassan Kazemian

¹PhD candidate, School of Computing and Digital Media, London Metropolitan University / CTI Renato Archer-DIMEC, Rodovia Dom Pedro I (SP-65), Km 143,6 - Campinas, SP, Brazil- ORCID[0000-0003-1644-3933]

² School of Computing and Digital Media, London Metropolitan University

Abstract: The paper proposes a novel index to classify how well UK Computer Science courses articulate cybersecurity related content through their course/module pages. The aim of this work is to raise awareness among British Universities to pay more attention to include and standardise cyber security content in computer science courses. Our results show that 80% of analysed courses scored 1 or 2-stars on a 5-Stars scale. The results also suggest the need of a formal delivery of cybersecurity content from the first year of the courses and possibly in a collaborative manner with the British Computer Society (BCS). To emphasize cybersecurity education in mitigating security lapses, the analogy is: it is better if most people know how to use a match than to train many fire-fighters.

Keywords: Cybersecurity Index, Computer Science, Undergraduate, Human Factors, Cyber Security Education, IT Education

I. INTRODUCTION

As reported in [1], we have two technological features threatening the global economy for the first time in a decade: i) cyber attacks and ii) data fraud. These two are within the top five most likely global risks such as natural disasters, extreme climate events and the failure to mitigate climate change. Technological threats are now recognized as an important theme and represent the first step towards improving security in cyberspace.

People are at the centre of all technology developments and their uses. Human factors do influence technological features and hence are the principal issues in this context. According to [2], understanding the requirements for the regional, national or accredited cyber security programs are necessary to ensure that there are identified benchmarks that are applied and are being met.

In USA, the National Security Agency (NSA) gives accreditation to Cyber Security courses that use the National Initiative for Cyber Security Education (NICE) Framework [3]. However, this is only for specific Cyber Security courses. In our research, we did not find similar accreditations for computer science courses, coherently, across a range of Universities globally.

In line with Higher Education Statistics Agency (HESA) [4], there were 79,480 students enrolled on Computer Science

courses in the UK in 2016/17. Whether UK undergraduate students are being prepared to develop cyber secure programs for the society was investigated in [5]. To do this, the authors analysed the curricula of UK computer science courses.

This work proposes a creation of an index to classify UK Universities by the relevance with which each institution offers cybersecurity content in their computer science courses. We didn't look specifically at cybersecurity courses. Rather, this work analyses the 'preparedness' of UK undergraduate students who are expected to develop software that meet baseline cybersecurity standards through their G400 courses [6].

II. LITERATURE REVIEW

A list of countries that plan to include compulsory learning of Computer Science in secondary education, highlights how this discipline is being taught at an increasingly earlier age. This list includes Austria, Australia, Finland, France, Germany, Ireland, Italy, Japan, Lithuania, Portugal, Republic of Korea, South Africa and Spain [7].

The European Commission has published a report that proposes three levels of knowledge on cybersecurity each student needs to know. These levels are: beginner, intermediate and advanced [8].

If the aim is to teach secure programming to the youngsters, it's necessary to make sure the future teachers of Computer Science are being prepared during their undergraduate courses and learn how to teach their future pupils about secure software development.

Conforming to Professors Moufida Sadok and Peter Bednar, an excessively technical focus is one of the main reasons why there are deficiencies in cybersecurity [9]. If technology is only a part of the problem, why does society pay so much attention to the technical side of the problem?

"While information security risks have involved and financial costs of cybercrime have increased, security practices and strategies have not adequately kept up with

dynamic and challenging attacks that are highly complex and difficult to detect.” [9]

Conversely, are security problems caused by the high costs of maintaining security?

Human factors are discussed by [10] and this work presents two cases on security incidents caused by human factors in two financial organizations. It also mentions the relevance of education in information security.

Privacy and cybersecurity issues and the pleaded (alleged?) solutions offered by software vendors [11] [12] [13] [14] [15] raise doubts about vendors’ promises. The privacy as advertised is hardly provided. Typically, they recommend the developers to explicitly alert the users of their products on the limitations of private browsing functionality. These papers testify how relevant the human factors are in the realm of the cybersecurity.

Surveys such as one carried out by the DSS Company [16] are very common and normally highlight special product features. Moreover, manufacturers often exaggerate what their solutions offer in terms of efficient protection and sometimes beyond the scope of achievable security. Parallely, knowing and exploiting these loopholes, hackers continue to attack vulnerable and high-profile institutions.

According to statistics from the Russian information security certification system, about one-third of the pieces of software tested exhibited vulnerabilities during a two-year study. According to [17], [18] and [19], it’s not known how failures can compromise information security and people’s privacy.

It is possible to confirm that attackers can gain full access to encrypted files, enabling credentials previously revoked, including TrueCrypt [20], VeraCrypt [21], GhostCrypt [22] and PGP Symantec Encryption Desktop [23].

When a trainee configures TrueCrypt or similar software for a business person, politician, high-ranking military or a researcher, installing the piece of software with the password “123”, the user is advised to change it to a “strong password” and share the password [24] [25] [26].

Personal credentials enter the e-commerce domain when a user buys flowers, food, vehicles and company-shares on the New York Stock Exchange, or takes part in home banking to pay bills and/or to make other bank transactions. When majority of common users are affected internationally, the scale is of global proportion.

The research in this field focuses on the treatment of user login information (usernames and passwords) by major service provider websites such as search sites, home banking, e-mail and e-commerce. In these cases, the focus is how clients input important personal details, and how these websites manage their users’ passwords.

In terms of security attacks, in Existential Forgery, an attacker can forge an authenticator for some unspecified user [27], which means that he/she cannot target one specific user. Whereas in Total Break, an attacker can recover the user key and can, therefore, build valid authenticators at his/her will.

As mentioned in [28], it’s important to analyse a vast class of information on the navigation activities that browsers save onto the hard-disk. Credentials were found in the form of clear text in non-volatile memory. This occurred with all browsers tested by the author of the mentioned paper.

Independent of the browser, Gmail, Amazon, eBay, Hotmail, and the Santander, Caixa and Citibank websites showed the similar vulnerability [29].

Investigations into cryptographic programs, web browsers and web credentials have shown that the credential management, security and privacy protection measures are currently quite poor. Meanwhile, investigations into “in-private navigation” show that the “privacy software” does not, in fact, gives adequate privacy to the user. Many researchers have focused on the technological aspects of the cases such as flaws in the code written or project errors. But, if vendors and users continue to manage credentials the way they are doing, it cannot be more vulnerable than a locked car with the car-key left in the door-lock. What can one expect from cybersecurity and privacy when many users and organisational practises are relaxed in protecting personal credentials?

“We use TrueCrypt in a corporate/enterprise environment. Is there a way for an administrator to reset a volume password or pre-boot authentication password when a user forgets it (or loses a key file)? Yes. Note that there is no ‘back door’ implemented in TrueCrypt. However, there is a way to ‘reset’ volume passwords/key files and pre-boot authentication passwords.” [26]

“If someone needs to access an encrypted file or a shared encrypted laptop, the encryption password will need to be shared, unlike your University password which should always be kept private. If you forget the encryption password for a file or USB stick, then the data will be inaccessible. In the case of laptops encrypted by the University, IT Services will store a recovery disk that will enable the laptop password to be reset.” [24]

In the same way when universities orient their pupils and users towards using “in-private” navigation, one has to stand still and review what is being taught about security and privacy [30] [31].

In [32], cybersecurity is classified in four categories: public, infrastructure, business and general. The basic message is to transform cybersecurity courses in a multidisciplinary direction. While this is laudable, broadening the knowledge of security experts do not solve the issue.

“From a socio-technical perspective, it is claimed that a viable system would be more user-centric by accommodating and balancing human process rather than entertaining an expectation of a one-sided change of behaviour of the end-user.” [9].

“Two reasons could potentially explain the poor effectiveness of the implemented security solutions and procedures: the boundary problem of risk analysis scope and the background of involved actors in risk assessment and security policy design.” [9]

Sadok and Bednar’s the work considers human-centricity as the best approach to address the cybersecurity problems.

It's necessary to adjust the whole background, specifically, the way cybersecurity and privacy are explained to the students. It proposes five units for High School programming courses in Israel: fundamentals, advanced programming, second paradigm, applications and theory. Likewise, [33] declares that security is among the key aspects in the field of computing.

Twenty-two years after the latter study, an interesting piece of research carried out in the US about teaching Computer Science in High School has suggested a new curriculum for teaching programming to teenagers [34]. Unfortunately, no security or privacy aspects have been considered so far.

In United States the national Centres of Academic Excellence in Cyber Defense Education (CAE-CDE) works with NSA to improve criteria to elevate the quality of cyber security education [35]. It presents three case studies of different institutions with different CAE statuses highlighting the importance of the CAE designation in enhancing cybersecurity education at these institutions. Unfortunately, all these studies and initiatives are about specialized cyber security undergraduate courses designed to prepare cyber security specialists.

In New Zealand, there have been discussions about Computer Science on the High School curriculum, albeit, without taking cybersecurity and privacy into account [35].

In the UK, researchers have been concerned with teaching Computer Science to produce more and more programming from the secondary level onwards [36] [37] [38].

“The challenge of introducing security in a sensible and useful manner can be addressed by considering the contextual perspectives”. [9]

However, the basis of cybersecurity must be introduced in early education, according to the Joint Task Force on Cybersecurity Education [39]. While this report provides guidelines for delivering cybersecurity education, all managers of technological courses could benefit from reading it.

The focus of our work is to suggest an index that demonstrates how cybersecurity is taught in Computer Science (G400) courses in the UK with the aim to emphasize its relevance and to foster improvement initiatives in the University curricula.

III. METHOD AND DATA COLLECTION

From the perspective that everything has a human element, the authors gathered information to understand what UK universities are thinking about cybersecurity and how students on relevant courses are being trained. For this, it was necessary to analyse the curricula of the offered courses. For that, it was decided to study the common basis of relevant course, disregarding cybersecurity specific courses. In particular, to understand the depth and breadth of cybersecurity related topics and their application, authors found Computer Science courses quite appropriate.

The authors considered the discipline components of 100 G400 Computer Science or similar courses [6], from the top 100 UK universities offering such courses as selected by the

ranks in “Webometrics Ranking of World Universities” - an initiative of the Cybermetrics Lab- a research group belonging to the *Consejo Superior de Investigaciones Científicas* (CSIC) being one of the largest public research body in Spain [41]. This ranking includes 280 UK universities. This study considers that the first 100 UK universities representing a sizable sample of the UK universities that offer some cybersecurity related content on their Computer Science or related courses

The title of the module or discipline and the content of the discipline as seen on Fig.1, Fig.2 and Fig3., when available online, were manually read line by line to identify cybersecurity content keywords such as security, privacy, cybersecurity, risk management, forensics, cryptography, safe software, safe programming, cybercrime, data protection, credential management and others security terms or expressions, or other contextualized elements that refer to cybersecurity enforcement.

Fig. 1 One of the best module descriptions founded.

Fig. 2 Security content in the module description.

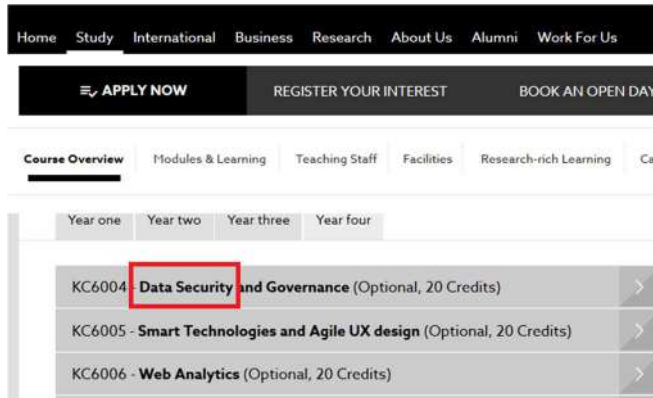


Fig. 3 Security content in the module title.

If a word or expression linked to security was found during the reading of a discipline's menu, it was scored as summarized in Table 1.

Annotations were made by the authors to identify at which point in time the security element was addressed, as well as whether the subject discipline was mandatory or optional.

The proposed Index of Relevance in Cyber Security (IRCS) privileges the mandatory content and the content given at the beginning of the course. The higher the mandatory content and the higher the content in the first year of the course, the higher the IRCS index as given by:

$$IRCS = \sum MC * 1 + \sum OC * 0.2 + \sum FYC * 1 + \sum SYC * 0.3 + \sum LYC * 0.15$$

Where,

MC = Mandatory content;

OC = Optional content;

FYC=First year content;

SYC=Second year content;

LYC=Latest year content.

Table 1-Collected data extracted by reading course descriptions provided by each institution on their website and classified by IRCS.

IRCS	University	OC	MC	Year		
				FYC	SYC	LYC
9,2	Robert Gordon University	0	8	0	0	8
5,1	University of Winchester	1	3	1	3	0
4,6	University of Liverpool	0	4	0	0	4
3,65	Lincoln University	1	2	1	1	1
3,45	Bangor University	0	3	0	0	3
3,45	University of Portsmouth	0	3	0	0	3
3,3	De Montfort University	0	2	1	1	0
3,3	University of Bedfordshire	0	2	1	1	0
3,15	University of Bradford	0	2	1	0	1
2,65	University of Kent	1	2	0	0	3
2,6	University of Derby	0	2	0	2	0

2,45	University of Reading	0	2	0	1	1
2,45	Edge Hill University	0	2	0	1	1
2,3	University of Oxford	0	2	0	0	2
2,05	University of Plymouth	5	0	0	2	3
2	University of Central Lancashire	0	1	1	0	0
2	Bournemouth University	0	1	1	0	0
2	London Metropolitan University	0	1	1	0	0
2	University of Abertay	0	1	1	0	0
2	University of Sunderland	0	1	1	0	0
1,9	Bristol University	3	0	1	0	2
1,9	Staffordshire University	3	0	1	0	2
1,65	University of Birmingham	1	1	0	1	1
1,65	University of Salford	1	1	0	1	1
1,5	University of Leeds	1	1	0	0	2
1,5	University of Ulster	1	1	0	0	2
1,5	University of Hertfordshire	1	1	0	0	2
1,4	University of Stirling	4	0	0	0	4
1,3	University of Cambridge	0	1	0	1	0
1,3	University of Exeter	0	1	0	1	0
1,3	Oxford Brookes University	0	1	0	1	0
1,3	University of Huddersfield	0	1	0	1	0
1,3	University of South Wales (Glamorgan & Wales Newport)	0	1	0	1	0
1,3	Teesside University	0	1	0	1	0
1,3	Birmingham City University (University of Central England)	0	1	0	1	0
1,2	Keele University	1	0	1	0	0
1,15	King's College London	0	1	0	0	1
1,15	Lancaster University	0	1	0	0	1
1,15	Aston University	0	1	0	0	1
1,15	Goldsmiths University of London	0	1	0	0	1
1,15	University of East London	0	1	0	0	1
1,15	London South Bank University	0	1	0	0	1
1,15	Cardiff Metropolitan University (University of Wales Institute Cardiff)	0	1	0	0	1
1,05	Loughborough University	3	0	0	0	3
1,05	Brunel University	3	0	0	0	3
1,05	City University London	3	0	0	0	3
0,7	Imperial College London	2	0	0	0	2
0,7	University of Southampton	2	0	0	0	2
0,7	Newcastle University Newcastle upon Tyne	2	0	0	0	2
0,7	University of Sheffield	2	0	0	0	2
0,7	Cardiff University	2	0	0	0	2
0,5	Kingston University London	1	0	0	1	0
0,35	University of Manchester	1	0	0	0	1
0,35	University of Warwick	1	0	0	0	1

0,35	University of Nottingham	1	0	0	0	1
0,35	Queen Mary University of London	1	0	0	0	1
0,35	University of Leicester	1	0	0	0	1
0,35	University of Saint Andrews	1	0	0	0	1
0,35	University of Surrey	1	0	0	0	1
0,35	Queen's University Belfast	1	0	0	0	1
0,35	The University of the West of England	1	0	0	0	1
0,35	Manchester Metropolitan University	1	0	0	0	1
0,35	University of Chester	1	0	0	0	1
0	University College London	0	0	0	0	0
0	University of Edinburgh	0	0	0	0	0
0	University of Glasgow	0	0	0	0	0
0	Durham University	0	0	0	0	0
0	University of York	0	0	0	0	0
0	University of Aberdeen	0	0	0	0	0
0	University of East Anglia	0	0	0	0	0
0	University of Sussex	0	0	0	0	0
0	University of Bath	0	0	0	0	0
0	University of Strathclyde	0	0	0	0	0
0	Heriot-Watt University	0	0	0	0	0
0	University of Essex	0	0	0	0	0
0	Swansea University	0	0	0	0	0
0	Royal Holloway University of London	0	0	0	0	0
0	Aberystwyth University / Prifysgol Aberystwyth	0	0	0	0	0
0	Cranfield University	0	0	0	0	0
0	Birkbeck University of London	0	0	0	0	0
0	University of Hull	0	0	0	0	0
0	Northumbria University	0	0	0	0	0
0	University of Brighton	0	0	0	0	0
0	Sheffield Hallam University	0	0	0	0	0
0	Liverpool John Moores University	0	0	0	0	0
0	Nottingham Trent University	0	0	0	0	0
0	University of Greenwich	0	0	0	0	0
0	Middlesex University	0	0	0	0	0
0	Coventry University	0	0	0	0	0
0	University of Westminster	0	0	0	0	0
0	University of Wolverhampton	0	0	0	0	0
0	Glasgow Caledonian University	0	0	0	0	0
0	Anglia Ruskin University	0	0	0	0	0
0	Napier University Edinburgh	0	0	0	0	0
0	Leeds Beckett University (Leeds Metropolitan University)	0	0	0	0	0
0	Canterbury Christ Church University	0	0	0	0	0
0	University of Bolton	0	0	0	0	0

0	University of Gloucestershire	0	0	0	0	0
0	University of Northampton	0	0	0	0	0
0	University of Worcester	0	0	0	0	0

IV. DISCUSSION

For simplicity, one may cluster (or group) the courses given in Table 1 on a 5-Stars scale as follows:

- 1 Star = IRCS <1
- 2 Stars = IRCS between 1 to 1,99
- 3 Stars = IRCS between 2 to 2,99
- 4 Stars = IRCS between 3 to 3,99
- 5 Stars= IRCS >= 4

54% of courses – 1 Star
26% of courses – 2 Stars
11% of courses – 3 Stars
6% of courses – 4 Stars
3% of courses – 5 Stars

In this work, we attempted to examine how well UK students on computer Science courses are exposed to mandatory cybersecurity content at the beginning of the course.

The apparent absence of anything about security and privacy in the curricula says a lot about the relevance of this theme on the courses in question. If cybersecurity content is not written into the discipline's syllabus, it is likely that it won't be taught formally and the consequences of this are potentially disastrous as emphasized in the literature review.

The heuristic analysis indicates that more than one-third of G400 courses in the UK leave cybersecurity as their mandatory curricula leaving cybersecurity as an optional discipline.

The first stage in the process of acquiring knowledge is to "remember" [44]. To remember something, one needs to be exposed to something new at an early stage with reinforced exposure carefully planned for the set duration.

Reflecting on [10], people are at the centre of any technological design and as mentioned by the author of [42], the education of cybersecurity content seems to be failing to attend the societal needs.

V. CONCLUSION AND FUTURE WORK

Based on our novel IRCS index for the sourced dataset, we concur to [46] [5] [44] in the sense that the best manner to make cyberspace safer is to teach cybersecurity to Computer Science students from the first year of the University as a mandatory content.

It is very desirable and important to have an evolved and more objective IRCS index to effectively measure the cybersecurity content in the Computer Science curricula. As a future work, we would like to derive robust IRCS by enhancing Table 1 with other scores such as professional certification or accreditation linked to the course. In addition,

we would like to automate the scoring with exhaustive keywords that can fully encompass the course and module webpages.

VI. REFERENCES

- [1] World Economic Forum, "Global Risks Report 2018," World Economic Forum, Geneva, 2018.
- [2] M. Dawson, "Hyper-connectivity: Intricacies of national and international," *Doctoral Thesis at London Metropolitan*, 2017.
- [3] D. Shoemaker, A. Kohnke and K. Sigler, *The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)*, Boca Raton: CRC Press, 2016.
- [4] HESA, "Higher Education Statistics Agency: UK, 2016/17," HESA, Promenade, 2018.
- [5] R. Ruiz, "A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, 2019.
- [6] Universities Central Council on Admissions, "Universities Central Council on Admissions," 2018. [Online]. Available: <https://www.ucas.com/ucas-terms-explained>. [Accessed 01 February 2018].
- [7] D. Passey, "Computer science (CS) in the Compulsory Education Curriculum: Implications for Future research," *Education and Information Technologies*, vol. 22, p. 401, 2017.
- [8] A. Ferrari, "DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe," European Commission Institute for Prospective Technological Studies, Seville, 2013.
- [9] M. Sadok and P. Bednar, "Understanding Security Practices Deficiencies: A Contextual Analysis. In S. Furnell, & N. Clarke (Eds.)," in *Human Aspects of Information Security and Assurance Conference Proceedings*, Plymouth, 2015.
- [10] A. Reza and H. J. a. A. A.-N. Shareeful Islam, "Analyzing Human Factors for an Effective Information Security Management System," *International Journal of Secure Software Engineering (IJSSE)*, vol. 4, no. 1, pp. 50-74, 18 9 2013.
- [11] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Opening the "Private Browsing" Data – Acquiring Evidence of Browsing Activities," in *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, 2014.
- [12] R. Ruiz, K. Park, F. Amatte and R. Winter, "Overconfidence: Personal Behaviors Regarding Privacy that Allows the Leakage of Information in Private Browsing Mode," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 4, no. 3, pp. 404-416, 2015.
- [13] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Tornado Pública a Navegação "InPrivate"," in *Proceedings of the IcoFCS2012*, Brasília - Brazil, 2012.
- [14] G. B. E. J. C. B. AGGARVAL, "An Analysis of Private Browsing Modes in Modern Browsers," in *Proceedings of the USENIX 2010*, 2010.
- [15] R. Ruiz, R. Winter, K. Park and F. Amatte, *Apoc@lypse: The end of antivirus*, North Charleston: North Charleston: CreateSpace Independent Publishing Platform, 2015, p. 134.
- [16] A. Filatov, "Data Security Solution," 25 02 2015. [Online]. Available: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress2014-arrowecs-roadshow-baltics>.
- [17] R. d. S. Ruiz, F. P. Amatte and K. J. B. Park, "Security Issue on Cloned TrueCrypt Containers and Backup Headers," in *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*, Kuala Lumpur - Malaysia, 2014.
- [18] R. Winter and R. Ruiz, "Corrosive Secrecy and Confidence: The Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security," *Cyber Security Review*, pp. 66-74, 01 03 2016.
- [19] R. Ruiz and R. Winter, "Lazarus: Data Leakage with PGP and Resurrection of the Revoked User," *Journal of Cyber Security and Mobility*, vol. 5, no. 2, pp. 1-14, 20 11 2016.
- [20] T. Foundation, "Truecrypt," 15 02 2013. [Online]. Available: <http://truecrypt.org>.
- [21] IDRIX, "VeraCrypt," 2018. [Online]. Available: <https://veracrypt.codeplex.com/>.
- [22] Ghostcrypt, "Ghostcrypt," 04 01 2018. [Online]. Available: <https://www.ghostcrypt.org/>.
- [23] Symantec, "Symantec Desktop Encryption User Manual," [Online]. Available: https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6205/en_US/symcEncrDesktop_103_win_usersguide_en.pdf?__gda__=1475850268_90925006947a919661523e2f67f5cea7. [Accessed 5 October 2016].
- [24] IT Services, The University of Manchester, "Encryption Software," 2014. [Online]. Available: <http://www.itservices.manchester.ac.uk/cybersecurity/advice/encryption/>.

- [25] University of Exeter, "Important Information for Users of TrueCrypt on Windows Laptops," 25 April 2014. [Online]. Available: <http://www.exeter.ac.uk/ig/infosec/encryptionforlaptops/usingtruecrypt/>.
- [26] Wake Forest University, "TrueCrypt install," 25 04 2014. [Online]. Available: <http://users.wfu.edu/yipcw/is/truecrypt/>.
- [27] K. S. K. F. N. FU, "Dos and Don'ts of Client Authentication On The Web," in *Proceedings of the 10th USENIX Security Symposium*, Whashington DC, 2001.
- [28] J. L. S. L. S. Oh, "Advanced Evidence Collection and Analysis of Web Browser Activity," *Digital Investigation*, pp. 62-70, 2011.
- [29] R. Ruiz, R. Winter, K. Park and F. Amatte, "The leakage of passwords from home banking sites: A threat to global cyber security?," *Journal of Payments Strategy and Systems*, vol. 11, no. 2, pp. 174-186, 2017.
- [30] University of Michigan, "Safe Computing," 01 September 2018. [Online]. Available: <https://www.safecomputing.umich.edu/beware/privacy/resources>.
- [31] Wake Forest University School of Business, "MSBA Software Installation," 2018. [Online]. Available: business.wfu.edu/msba-software.
- [32] R. B. Ramirez, Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization, Cambridge: Master's thesis in technology and policy, Massachusetts Institute of Technology, 2017.
- [33] J. Gal-Ezer, C. Beeri, D. Harel and A. Yehudai, "A High-School Program in Computer Science," *Computer*, vol. 28, no. 10, pp. 73-80, 1995.
- [34] G. Alexandron, M. Armoni, M. Gordon and D. Harel, "Teaching Scenario-based Programming: An Additional Paradigm for the High School Computer Science Curriculum, Part 1," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 58-67, 2017.
- [35] P. Wang, M. Dawson and K. L. Williams, "Improving Cyber Defense Education Through National Standard Alignment: Case Studies.," in *National Security: Breakthroughs in Research and Practice*, edited by Information Resources, Management Association, IGI Global, 2019, pp. 78-91.
- [36] T. Bell, P. Andreae and L. Lambert, "Computer Science in New Zealand High Schools," Brisbane, 2010.
- [37] N. C. C. BROWN, S. SENTANCE, T. CRICK and S. HUMPHREYS, "Restart: The Resurgence of Computer Science in UK Schools," *ACM Transactions on Computing Education (TOCE)*, vol. 14, no. 2, p. 9, 2014.
- [38] N. C. C. Brown, M. Kölling, T. Crick, S. P. Jones, S. Humphreys and S. Sentance, "Bringing Computer Ccience Cack Into Schools: Lessons From The UK," Denver, 2013.
- [39] S. Sentance, M. Dorling, A. McNicol and T. Crick, "Grand challenges for the UK: upskilling teachers to teach computer science within the secondary curriculum," Hamburg, 2012.
- [40] ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, "Cybersecurity Curricula 2017," ACM; IEEE-CS; AIS SIGSEC; IFIP WG 11.8, New York, 2017.
- [41] Cybermetrics, "Webometrics," 2018. [Online]. Available: <http://www.webometrics.info>. [Accessed 04 02 2018].
- [42] B. (. E. M. F. E. H. W. K. D. Bloom, Taxonomy of Educational Objectives, Handbook I., Allyn & Bacon ed., New York: Pearson, 1956.
- [43] J. M. Pittman and R. E. Pike, "An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp," *Information Systems Education Journal*, vol. 4, no. 3, pp. 4-13, 13 5 2016.
- [44] N. Ruiz, P. Shukla and H. Kazemian, "Privacy in The First Line of the First Code," 17 04 2020. [Online]. Available: <https://science.sciencemag.org/content/317/5842/1178/tab-e-letters>. [Accessed 27 04 2020].

Method and Tool for Generating Table of Relevance in Literature Review (MTTR)

Dr Natasha Ruiz¹, Rogério Winter², Dr Ferruccio de Franco Rosa³, Dr Pancham Shukla⁴, Prof. Dr Hassan

Kazemian⁵

^{1,3} DIMEC/CTI-Renato_Archer -Brazilian Ministry of Science, Technology, Innovation and Communications, Campinas,

² FEEC/UNICAMP, Campinas, Brazil

³ UNIFACCAMP, Campinas, Brazil

^{1, 4, 5} Intelligent Systems Research Centre, School of Computing and Digital Media, London Metropolitan University, London, UK

¹ natashasruiz@outlook.com; natasha.ruiz@cti.gov.br

² rogwinter@gmail.com

³ ferruccio.rosa@cti.gov.br

⁴ p.shukla@londonmet.ac.uk; spancham@yahoo.com

⁵ h.kazemian@londonmet.ac.uk

Abstract— Every day, researchers in computing and IT are challenged with several articles that they need to rate, classify and separate quickly and effectively to contextualize and further advance their research effectively. It is considered that literature review is the most important step of discovery. Notably, a literature review is a part that allows the researcher to adjust the perspectives and limitations of an area of study. However, there is a lack of effective methods and tools for this activity. Often, traditional knowledge management techniques result in the “Gordian Knot” slowing down the process of literature review considerably.

In this article, we present a Method and Tool for Generating Table of Relevance in Literature Review (MTTR). The MTTR is an innovative organizing method supported by software tools that make the literature review activity more efficient, faster and cheaper. An interesting feature of MTTR is data visualization using the Heat Map technique, Word Cloud and statistical techniques in designating and comparing each scientific article with the other relevant articles. The productivity gains in MTTR occur due to the automation in structuring and sorting scientific articles. In addition to efficiency, the lowest cost has the potential to place the MTTR as a preferred tool for the researcher. The anecdotal evidence reported in this article suggests that it is possible to carry out a literature review in a much shorter time with MTTR than in the traditional manner.

Keywords: Review Method, Heat Map, Word Cloud, Active learning tools, Systematic Review

1 Introduction

A literature review is a careful selection of relevant literature to understand the research background and the context of the problem. It allows appreciation of the earlier studies and contributions of other researchers in the field. It also consolidates the basis in which the logic of intellectual research is being structured and helps to open new avenues of unexplored terrain. In the domain of knowledge management and curation, there are many articles that discuss methods to improve and ease the selection and prioritization of the processes for systematic (Biolchini *et al.*, 2005; Budgen and Brereton, 2006) or quasi-systematic literature reviews (Da Silva *et al.*, 2017). Automated or semi-automated literature review protocols and processes consist of parameters such as bases and indices; search phrases; inclusion and exclusion criteria; and extracts of synthesised or preliminary analysis of the works being available in the pool. Despite variations in format, style and emphasis, the literature review surveys usually have a basic structure such as: Title, Abstract, Keyword, Introduction, Method, Discussion, Conclusion, and References. In general, the structure of the research paper is a subjective and imprecise model as it is based on researchers’ diverse preferences of drafting, reading, interpreting, and organising the content under consideration. Hence, many literature review processes and tools are susceptible to various errors and a considerable amount of time in classifying the articles. Despite being tedious and complex, efficient development of the protocols and processes for the literature review of a large number of scientific articles are necessary to further advance the existing knowledge in any discipline. The Heat Maps are

important visualization tables for viewing and interpretation of data. Since they add relevance factor (Whetten, 1989), they are used in various methods presented in (Laura M. Stapleton University of Maryland, 2008). In study of multidisciplinary cooperation, a way to value the science of computation provided by (Surveys, 1994) mentions the generation of tools to support research in other areas such as generating new ideas, designs and tools for task assignment, information routing, and group decision-making. In simple terms, adding or subtracting some factor from an existing model may be sufficient for a novel theoretical framework (Whetten, 1989).

This work proposes a novel method - Method and Tool for Generating Table of Relevance in Literature Review (MTTR) intended as a support tool for systematic and non-systematic reviews (Figure 1) following the complete cycle between acquisition of relevant articles and ending with visualization through the heat map (Figure 3). The proposed method exploits the content of the key sections (e.g. Title, Abstract, etc.) of the set of sample papers to generate the word clouds in selecting and organizing the related research works. The heat map shows how much any word or expression appears in each article and produces a relevance table as an indicator for prioritizing and ordering the selected works in terms of 'meaningfulness' in the literature review. In particular, the emphasis is on an improved objective criteria that use counting of words and expression in the text to provide the relevance of each article into a heat map. MTTR offering accurate determination of the relevance of articles to a search presents advantages such as: drastic reduction in article review time, data visualization using a heat map, unequivocal indication of the relevance of the evaluated articles, rapid search refinement, improvement in the quality of the analysis and objective classification of articles. Compared to other methods presenting subjective results, deficient or incomplete interpretation, and excessive time, the results presented by the MTTR are objective, measurable and repeatable. In summary, the main contributions of this research are: i) the method for generating relevance tables in literature review (MTTR) as shown in Figure 2; and ii) a software tool for supporting MTTR.

The remainder of this paper is organized as follows: Section 2 provides Literature Review; Section 3 presents a summary of related work; Section 4 outlines conceptual architecture of MTTR and related concepts; and finally in Section 5, we present our conclusions and future work for the MTTR.

2 Literature Review

The literature review is the process of searching, analysis and description of a body of knowledge in quest of an answer to a specific question. The systematic review process can be understood as a three-step approach as follows (Biolchini *et al.*, 2005):

- The first phase begins from the concepts that formally represent the problem in question, make it explicit. It encompasses the study of works that can provide evidence on the specific topic of research;
- In the second phase, works are detailed or categorized according to their content and compared in a systematic manner with to identify results or trends that that can be analysed;
- The third phase begins with the results of the previous phase and focuses on the analysis and synthesis to reach the conclusions.

Regardless of the phases of the literature review, researchers are expected to look at all the relevant material such as books, journal articles, newspaper articles, historical records, government reports, theses, dissertations written on the topic of interest.

On the subject of literature review specific to the area of computer science, particularly Software Engineering, the guidelines of (Biolchini *et al.*, 2005) assist researchers on "what" rather than "how " when it comes to engaging in methods and techniques for literature review. (Bond and Acheson, 2017) present the literature review as a mandatory step in scientific work. The theme of the work addresses systematic review in Health Sciences. The objective is to evaluate, summarize and communicate the results and their implications. Despite all the guidelines contained in the article, the researchers need to go through all the steps of the literature review manually.

The article written by (Miley and Read, 2011) examines students response to a technique for summarizing available information based on word frequency. The article reports students' experience with the technique of creating 'word clouds' to enhance personal and small group study. The survey result indicates that it is

accommodative of students' learning style preferences. Kolb's learning styles inventory was used. The research also found that word clouds have potential in the workplace and that students enjoy using word clouds and it a potential learning tool. (Ennis, 2010) explores the use of word clouds for abstracts as indicators of documents content in an academic context. The author identifies current uses for abstracts, issues in their production, and the use of Web 2.0 technologies as content indicators. Author considers a survey of six participants who completed questionnaires to determine their initial impressions of abstracts, before viewing multiple word cloud summaries and filling out additional questionnaires about the usefulness of those summaries. It advocates that word clouds are useful indicators of document content that help researchers to decide whether an article is relevant to their research topic. It shows that large clouds were preferred by participants over clouds with fewer words. The research found that clouds are useful and quick to create, they are relatively inexpensive, they can be used as document summaries in place of traditional narrative summaries. The article by (Reyes-Foster and DeNoyelles, 2016) presents exploratory research on the influence of word clouds on students' critical thinking when they are incorporated into online discussions. In an online discussion, students were asked to critically analyse two speeches, with the task assigned under two conditions: one in linear text format and the other the text was presented in the form of word clouds. Students who observed the word cloud exhibited more instances of critical thinking than students in the linear text reading condition. The article concludes with recommendations for other educators to use the word cloud in similar approaches.

(Vieira, Vieira and Coelho, 2019b) proposed a data-driven approach to developing a taxonomy on a data structure in a list of triple bottom line (TBL) metrics. The approach is built on the authors' reflection on the subject and a review of the literature on TBL. The predicted taxonomy framework grid developed through this approach allows existing metrics to be sorted, grouped, and standardized. The reported approach aims to develop a taxonomic structure that can be seen as a two-dimensional table, focused on characteristic questions and on the characterization of responses. The method proposed in (ACM, 2019) as seen in Table 1 adds a further dimension to the concept matrix to handle the unit of analysis after the interpretation of a number of papers. The distribution provided by search engines in ordering the papers in consolidating the literature review was proposed in (Webster and Watson, 2014). In Table 1, we can observe three concepts: O = Organizational; G = Group and I = Individual. The criteria to classify each paper into this concept depends on the subjective interpretation of the reader.

Table 1 – Table that adds a further dimension to the concept matrix to handle the unit of analysis

Concept Matrix Augmented with Units of Analysis												
Articles	Concepts (Organizational; Group; Individual)											
	A			B			C			D		
Units of Analysis	O	G	I	O	G	I	O	G	I	O	G	I
1					X			X				X
2	x				X	X		X				
...								X	X		X	

Table 2 - Example paper's table to show the paper's contribution in a survey paper

Summary of the main references and contributions													
LEGEND: A = Paper Reference; B = Performance; C = Reputation; D = Security design; E = Recommendation; F = User context aware; G = Contractual guarantees; H = Certification; I = Resources involved; J = Transparency; K = Information Disclosure (security incidents); L = Domains; M = Contribution type													
Id	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Alhanahnah, et al. (2018)[5]	X	X	X				X		X		GV, IS	Taxonomy
2	Kanwal, et al. (2015) [6]					X	X	X		X		IS	Taxonomy
3	Lansing, et al. (2016)[21]	X	X	X		X	X	X				GV, IS	Taxonomy
4	Chrysikos, et al. (2018) [7]		X	X	X	X			X			IS	Taxonomy, Framework
5	Dasgupta, et al. (2011) [32]			X		X	X					GV	Framework

In the article (A. B. Filho, F. de Franco Rosa, R. Ruiz, 2019), authors summarize a manual survey as implemented in Table 2 of word clouds from 39 papers. This process did take three full days of work. The reading and interpretation to mark the papers' contribution in columns B to K were also dependent on the subjective interpretation of the reader.

The proposed method aims to show usefulness of a combination of automatic or semi-automatic ways of exploration and presentation of the literature review to assist the researchers effectively.

3 Related Works

The analysis of the complex survey was dissected in several aspects in (Laura M. Stapleton University of Maryland, 2008). Since the criteria for the formulation of the questions, the composition of the data from the dataset, and sampling design, the tables are essential for viewing and interpretation of data and they are used in various methods presented in (Laura M. Stapleton University of Maryland, 2008). Most of the work dealing with the theme survey is focused on questionnaires that will be answered by humans in interview or structured and standardized as numbers, economic indices, or census data. When we talk about a survey of scientific literature review, we still encounter subjectivity, even in tables. As the columns are defined by the subjective criteria by the author, the answers that match article criteria are very dependent on the individual interpretation of the reader.

In (Fowler *et al.*, 2014), the authors argue that the research methodology seeks to identify principles on research design, collection, processing and analysis and are linked to the cost and quality of research estimates. In short, this means that research methodology focuses on improving the quality of output within cost constraints, or alternatively reducing costs to some fixed level of quality. (Fowler *et al.*, 2014) argue that in high-quality research, in addition to the methodological and scientific aspect of the questionnaires used, care must be taken in the selection of statistical samples and the universe surveyed. The didactic reading of the text is a function of the layout, analysis and comparisons, and the presentation of surveys and data tables (Figure 1). In Figure 1, the method presented is unidirectional whereas our method is cyclic (Figure 2). In our work, the table is not only a dataset but a representation of the analysis of the data collected. In fact, our method aims for an automation, objective analysis, and pragmatic applications by transforming the conventional methods based on manual and subjective approaches.

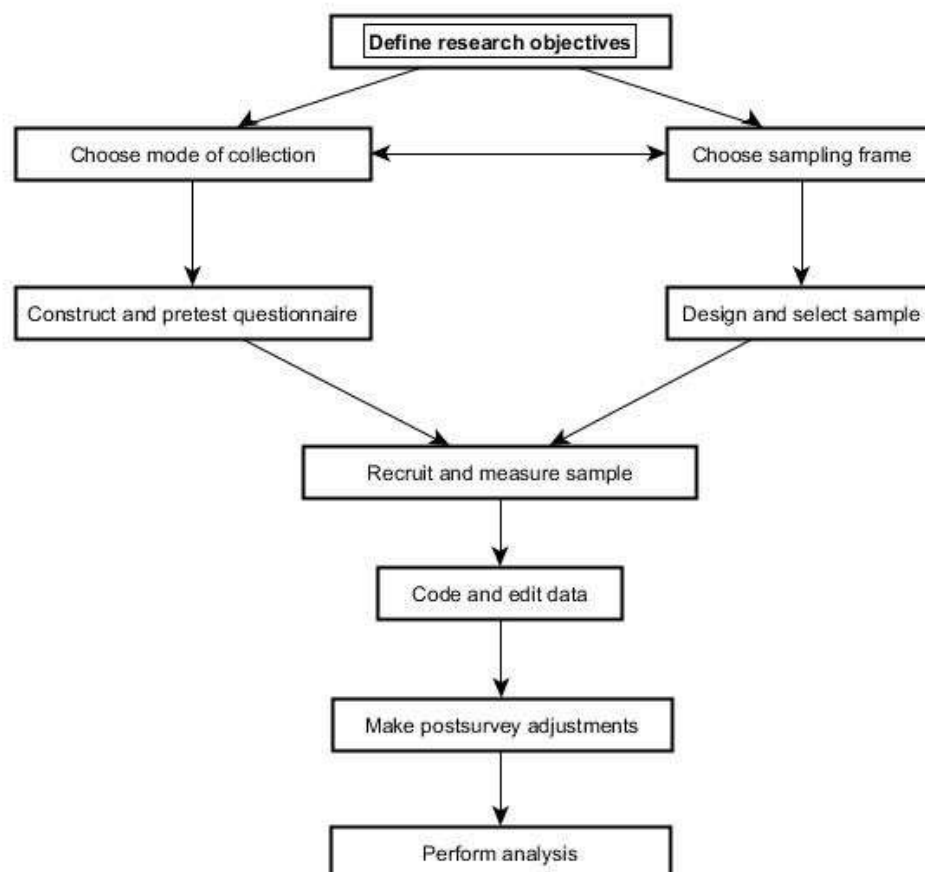


Figure 1 A survey from a process perspective

4 Conceptual Formalization

Based on the articles presented in Section 2 (Literature Review) and Section 3 (Related Works), we developed a Method and Tool for Generating Table of Relevance in Literature Review (MTTR) to provide better performance and reliability to researchers during their literature review tasks. The core aim of MTTR is to drastically reduce the time for literature review compared to other table based traditional methods. MTTR methodology tries to mechanise the usual logic of conducting the literature review through steps that allow the researcher to efficiently automate and direct the work. MTTR allows the researcher to obtain relevant cues from a large number of articles those that are directly linked to the main interest.

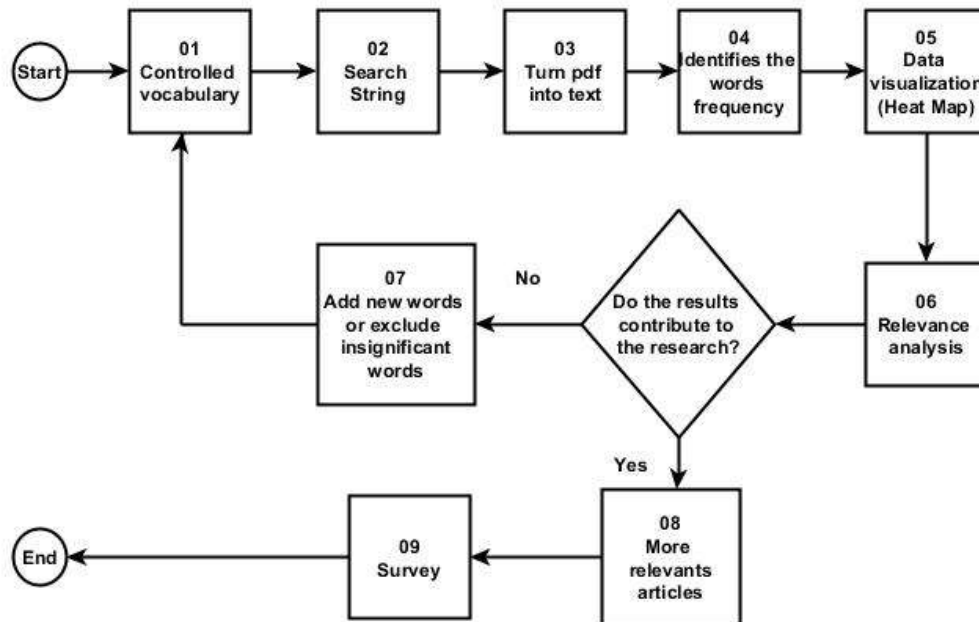


Figure 2 Process of MTTR

The process of MTTR of shown in Figure 2. This process can be seen as acquiring text files of relevant papers and ending with the taxonomy table. To work with MTTR method in a personalised manner, the researchers can adopt database-based solutions such as use of separate folders to store PDF papers, spreadsheets to organize the content or other third-party software of their choice. The MTTR is elaborated in nine steps as follows:

- **Step one** - Define controlled vocabulary, i.e., definition of the Title of the Survey.
- **Step two** - Define a search string, i.e., a priori. The researcher already has a research idea and needs to define a search string that will be used in searches of different scientific article databases (IEEE, ACM, SPRINGER, RESEARCHGATE, ACADEMY). The search string will help find potential articles useful for the search.
- **Step three** – Convert PDF to text. In order to carry out the work of establishing the relevance of the words, the articles are converted from PDF format to plain text, excluding images and tables. The result is stored in the MTTR database.
- **Step four** - Identify the word frequency. In this step, the MTTR performs the automatic counting of the frequency of words and expressions in each article that the researcher selected. We developed a Python algorithm that performs statistical operations and does automatic counting of words and expressions. In this way, a dataset containing words and expressions in each article is generated. This is a necessary step in order to ensure the process proceeds to the Word Cloud Generation (Figure 3). As discussed earlier, the word cloud makes it easy to see the relevance of words.
- **Step five** - Heat Maps. The words generated in the previous step are used for the integration and visualization of the most important words and expressions. The data is transformed into word clouds and heat maps (Figure 4) for each article to enable more efficient analysis. The visualization of information through the heat map helps the researcher to adjust the search expression and to select relevant articles.

- **Step six** - Relevance analysis. It exploits definition of expression dictionary based on the results of the previous items and the intent and point of view of the researcher.
- **Step seven** - Add or exclude terms. Each new 'term item' needs to be linked to the word dictionary;
- **Step eight** - Selection of relevant papers. Analysis and attribution to rate each paper for individual word clouds item on the scale of 1 to 5 according to the relevance of word cloud of the individual paper in comparison of all word clouds.
- **Step nine** – Write the survey. Summarize a short paragraph for each paper to describe the paper resulting into the Survey topic; create introduction topic; generate heat map of classification of each paper; create discussion topic including the table; create a brief of this method and cite it; create conclusions; create references; format the survey paper.



Figure 3 Word cloud

	cyber	security	system	information	mission	network
articles						
02-DesigningMethodDiscoveringExpertise.txt	203	238	222	390	2	55
23-Cyber-ARGUS - A mission assurance framework.txt	0	73	115	91	200	0
18-frameworkfortheethicalimpactassessment.txt	0	13	13	93	0	16
62-Mission-Centric Automated Cyber Red Teaming.txt	87	56	65	0	153	84
21-UnderstandingInformationAssuranceSecurity.txt	0	313	89	350	1	9
20-Fundamental Concepts of Cyber Resilience.txt	149	18	228	14	9	107
36-The Human Factor in Cybersecurity.txt	229	58	72	55	5	51
25-Simulations in Cyber-Security.txt	110	101	43	30	0	122

Figure 4 – Partial view of heat map of 56 papers, 46 terms, and their relevance for each word.

Table 3 Main contributions and a conceptual characterization

Reference	Main Contribution		Software				Performance	
	Concepts	Method	Word cloud	Heat map	word statistics	Summarization	Low	high
(Biolchini <i>et al.</i> , 2005)	Yes	Yes	No	No	No	No	Yes	No
(Borja, no date)	Yes	Yes	No	No	No	No	Yes	No
(Whetten, 1989)	Yes	Yes	Yes	No	No	No	Yes	No
(Bond and Acheson, 2017)	Yes	Yes	No	No	No	No	Yes	No
(Miley and Read, 2011)	Yes	Yes	Yes	No	No	No	Yes	No
(Ennis, 2010)	Yes	Yes	Yes	No	No	No	Yes	No
(Vieira, Vieira and Coelho, 2019a)	Yes	Yes	Yes	No	No	No	Yes	No
(Reyes-Foster and	Yes	Yes	Yes	No	No	No	Yes	No

- **Step three** – Convert. We use *pdftotext* for this task. The *pdftotext* is a command line utility that converts PDF files to plain text.
 - **Step four** - Identify the word's frequency. We developed an algorithm in Python, which is responsible for reading files in text format and categorizing keywords and expressions. For a better understanding of the text, we provide a heat map (Figure 4) with the inferred contribution of each work in the literature review.
 - **Step five** - Heat Map. Words and expressions are loaded directly into an excel spreadsheet for viewing via the heat map. The algorithm also produces the word clouds as shown in Figure 3.
 - **Step six** - Relevance analysis. Heat map and word clouds makes it possible to identify the most relevant words and the most relevant articles in the search.
 - **Step seven** - Add or exclude terms. This is a recursive step where the researcher will make the necessary adjustments.
 - **Step eight** - Selection of relevant papers. The process allows list control by inputting a fixed number (N) to list N most important articles for the given research topic.
 - **Step nine** – Write the survey. After selecting the most relevant articles, it is time to write the survey. Text Compactor - a free online automatic text summarization tool was use for that purpose.
- After MTTR, We found an experience author to subjectively articulate percentage of relevance for each article. What we found that the practice of fully manual reading and classification, where an article whether meets or does not meet the criteria, is bases on the subjective perception of the author. As shown in the articles, several papers have a cloud of words for easy visual identification of topics discussed. The researcher needs to work on the spreadsheet to classify, summarize, define colours grades and cosmetic aspect of the heat map shown in Figure 4. It was valuable to consider some kind of groups or taxonomy. In our example in Figure 5, the reader can quickly identify three elements for reflection:

- a) The top papers by subject from top to bottom in a table;
- b) Subjects most researched starting from the left side to the right side;
- c) Fields and Subjects free and unexplored that can be new opportunities for study. (See the right side of the table in red colour)

6 Conclusion and future perspective

The proposed MTTR work attempts to change the current logic in conducting a literature review by automatic counting the frequency of words in the articles. The generation of the dataset containing every word of every article reviewed, interpreting the dataset, and turning it into a heat map and word clouds for each article allows greater efficiency in the analysis. Our method uses word clouds associated with a table that shows the gradient of colours indicating the relevance of the key words found in articles closely aligned to the research topic. Compared to other traditional methods, our method has the advantages such as objective classification of articles, significant reduction in the runtime of the literature review, visualization of results, quick search and refinement in listing of the relevance of articles. The proposed method permits structured analysis of many relevant papers and enables personalised innovation and creativity of the researcher for each survey. In summary, MTTR archives: i) significant reduction of time for article selection and classification; ii) heat map based visual indicator of the relevance of the literature; and iii) an objective criterion of classification that permit to repeat and reproduce the same results. The MTTR was used in the article (Winter *et al.*, 2020) which allowed the approval of the event ITNG 2020 and in this real example, it reduced the bibliographic review execution time by 95% compared to a similar article produced by the authors (Amândio Balcão Filho; Ferrucio de Franco Rosa; Rodrigo Ruiz; Rodrigo Bonacin; Mario Jino, 2019) in the traditional format.

Our short-term perspective is to make the MTTR freely available to students and researchers who need to review the literature for academic work. This will help as obtain practice-based feedback to further enhance and automate our method.

7 References

A. B. Filho, F. de Franco Rosa, R. Ruiz, R. B. and M. J. (2019) 'A study on Trust Models in Cloud Computing', in

ASE/IEEE (ed.) *16th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2019*. Abu Dhabi.

ACM (2019) *ACM Master Article Template*.

Amândio Balcão Filho; Ferruccio de Franco Rosa; Rodrigo Ruiz; Rodrigo Bonacin; Mario Jino (2019) 'A study on Trust Models in Cloud Computing', in ASE/IEEE (ed.) *16th ACS/IEEE International Conference on Computer Systems and Applications AICCSA 2019*. Abu Dhabi.

Biolchini, J. et al. (2005) *Systematic Review in Software Engineering, Engineering*. Rio de Janeiro. doi: 10.1007/978-3-540-70621-2.

Bond, C. and Acheson, C. (2017) *Student Learning Development University of Otago*.

Borja, A. (no date) *11 steps to structuring a science paper editors will take seriously*, Elsevier Connect.

Ennis, A. (2010) *Indicators of Content : the role of word clouds in the creation of summaries*. Loughborough University.

Fowler, F. J. et al. (2014) *Survey Methodology Established in part by WALTER*. Edited by Wiley. Wiley.

Groves, R. M. et al. (2004) *Questions and answers in surveys, Survey Methodology*.

Laura M. Stapleton University of Maryland, B. C. (2008) 'Analysis of Data from Complex Surveys', in Erlbaum Associates, L. (ed.) *International Handbook of Survey Methodology*. 1st edn. New York: Taylor & Francis Group, LLC, pp. 342–369.

Miley, F. and Read, A. (2011) 'Using Word Clouds to Develop Proactive Learners', *Journal of the Scholarship of Teaching and Learning*, 11(2), pp. 91–110. Available at: <http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ932148&site=ehost-live>.

Reyes-Foster, B. M. and DeNoyelles, A. (2016) 'Influence of Word Clouds on Critical Thinking in Online Discussions: A Content Analysis', *Journal of Teaching and Learning with Technology*, 5(1), pp. 16–32. doi: 10.14434/jotlt.v5n1.13805.

Da Silva, M. B. D. et al. (2017) 'Public ICT governance: A quasi-systematic review', *ICEIS 2017 - Proceedings of the 19th International Conference on Enterprise Information Systems*, 2(Iceis), pp. 351–359. doi: 10.5220/0006314603510359.

Surveys, A. C. M. C. (1994) 'Thomas W. Malone and Kevin Crowston *', *ACM Computing Surveys*, 26(1)(March), pp. 87–119.

Vieira, F. L., Vieira, P. A. and Coelho, D. A. (2019a) 'A data-driven approach to development of a taxonomy framework for triple bottom line metrics', *Sustainability (Switzerland)*, 11(9). doi: 10.3390/su11092717.

Vieira, F. L., Vieira, P. A. and Coelho, D. A. (2019b) 'A Data-Driven Approach to Development of a Taxonomy Framework for Triple Bottom Line Metrics', *Sustainability*, 11(9), p. 2717. doi: 10.3390/su11092717.

Webster, J. and Watson, R. T. (2014) 'ANALYZING THE PAST TO PREPARE FOR THE FUTURE : WRITING A REVIEW', *MIS Quarterly*, 26(2).

Whetten, D. A. (1989) 'What Constitutes a Theoretical Contribution?', *Academy of Management Review*, 14(4), pp. 490–495.

Winter, R. et al. (2020) 'Cyber Mission Operations: A Literature Review', in *17th International Conference on Information Technology: New Generations*, pp. 31–37. doi: 10.1007/978-3-030-43020-7_5.

Dr Natasha Ruiz is PhD in Computer Science at Intelligent Systems Research Centre, School of Computing and Digital Media, London Metropolitan University, London, UK and cybersecurity and privacy researcher at CTI Renato Archer, Brazilian Ministry of Science and Technology.

Rogério Winter is a retired Brazilian Army Colonel with extensive experience in cyberwarfare, cybersecurity and electronic warfare. He obtained his Master's degree in electronic engineering and computation in the Aeronautics Institute Technological (ITA-Brazil) and he is a PhD candidate at University of Campinas (Unicamp – Brazil). Today, Rogério is director in the HRW Tech.

Dr Ferruccio de Franco Rosa is Dr. in Electrical Engineering (UNICAMP, Brazil). He is a Senior Researcher at the Renato Archer Information Technology Centre and a Professor at the UNIFACCAMP, in the Master's Program in Computer Science. He was Head of the Information Systems Security Division. He has experience in software engineering, specifically in software assessment.

Dr Pancham Shukla received his PhD in Electrical and Electronic Engineering from Imperial College London. He is a Senior Lecturer in the School of Computing and Digital Media at London Metropolitan University since

2007. He is a Deputy Director of Communications Technology Research Centre and a Vice-Chair of School's Research Students Progress Group.

Prof Dr Hassan Kazemian is BSc Engineering (Computing) UK, MSc Computer Control Systems Engineering UK, and PhD in Applications of Artificial Intelligence to Robotics UK. Full Professor in Artificial Intelligence, Director of Intelligent Systems Research Centre at School of Computing and Digital Media of London Metropolitan University. Also Fellow (FIET), (former FIEE), (FBCS), Engineering Council and (EPSRC).